CHAPITRE 8

LA PROTECTION DU SECRET DANS UNE SOCIÉTÉ D'INFORMATION

La France, comme les autres pays industrialisés, a connu dans les cinquante dernières années une transformation très rapide et très profonde de son économie, de ses modes de vie et de ses valeurs. Cette transformation – que certains ont analysée comme le symptôme d'un véritable changement de civilisation – est due, pour l'essentiel, aux conséquences du progrès technique considérable de la seconde moitié du XX^{e} siècle, progrès qui a tout à la fois modifié en profondeur les comportements et permis l'émergence d'un nouveau type d'économie, fondée sur l'utilisation intensive des technologies de pointe et des ressources d'information à l'échelle internationale.

Ce contexte dominant a nécessairement des retombées sur les formes et les moyens du contre-espionnage. En effet, tout le dispositif de protection du secret et de défense de l'État est un processus intimement lié, d'une part, à l'appréciation de ce qui est stratégique pour le développement et la défense d'une collectivité à un moment donné et, d'autre part, à l'état des moyens de communication et de traitement de l'information disponibles dans cette société. Le développement d'une économie internationale de l'information postindustrielle et technologique, fondée essentiellement sur le primat de la communication et développant des nouvelles formes de richesse sur une base supranationale, modifie donc fondamentalement la valeur des principaux paramètres de l'équation du secret.

Trois caractéristiques, en effet, décrivent synthétiquement cette modernité [1] :

– la diversification des facteurs de puissance. Face aux facteurs traditionnels de la puissance politique, diplomatique et militaire, les enjeux de puissance et les luttes stratégiques se déplacent vers des éléments, souvent demeurés secondaires dans le passé, tel le facteur économique, technologique ou culturel;

– la diversification des acteurs de puissance. À côté des États, d'autres acteurs pénètrent dans les jeux de la concurrence et de la puissance, à

[1] Cf. Bertrand Warusfel & Patrick Folléa, « Contribution à une réflexion sur les stratégies indirectes », *Stratégique*, Fondation pour les Études de défense nationale, 1987, n° 4, pp. 39 et s.

supranationales issues de la « société civile », qui viennent contester aux États leur monopole stratégique ;

– la transformation des lieux et des supports de la puissance. À l'ancien ordre basé sur la territorialité (frontières, espaces) et la matérialité du pouvoir et de la richesse (appropriation physique des ressources et des territoires), la nouvelle donne oppose la délocalisation de la puissance et l'immatérialité des ressources informationnelles, passant ainsi d'une logique d'appropriation des stocks à celle du contrôle des flux.

Appliqué au système de protection du secret, on peut décrire trois transformations complémentaires, caractéristiques de la *« société d'information »* contemporaine : la mutation du contenu du secret qui tend à couvrir de plus en plus d'informations de nature technologique ou économique, celle des acteurs de la protection de ces secrets, qui sont de plus en plus souvent des personnes privées soumises à des logiques autonomes et celle – enfin – des moyens et supports du secret, qui sont essentiellement aujourd'hui des systèmes d'information.

LA MUTATION DE L'OBJET DU SECRET : LA DIFFICILE PROTECTION DES SECRETS ECONOMIQUES ET TECHNOLOGIQUES

Dans une société où l'information est, non seulement, largement diffusée par les moyens de communication, mais aussi la source dominante de la richesse et du pouvoir, le statut du secret apparaît, plus que jamais, fondamentalement ambigu. Plus l'on communique, plus l'information devient importante ; donc, le secret devient de plus en plus utile pour la protéger, avec pour conséquence paradoxale que plus le niveau de communication augmente, plus le secret devient à la fois nécessaire (pour sauvegarder la valeur de l'information) et intolérable (puisque contraire, par nature même, à la logique de la communication).

Cette contradiction est, notamment, visible aujourd'hui dans le fait qu'au moment où la sphère du secret paraît se rétrécir devant la croissance de l'information ouverte, les contraintes des nouvelles rivalités de puissance poussent à inclure dans ce champ du secret des données économiques et technologiques jusqu'alors peu protégées.

Or, malgré l'affirmation du caractère global de la défense nationale par l'ordonnance du 7 janvier 1959 et les modifications successives du Code pénal en 1939 et 1960, les secrets économiques et technologiques ont toujours été difficilement protégés par le secret de défense et ont plutôt profité de certaines protections « périphériques ».

Des secrets économiques et technologiques mal pris en compte par le secret de défense

Nous avons remarqué précédemment que la jurisprudence était restée très réservée quant à l'utilisation du secret de défense pour protéger des informations économiques ou technologiques et avait le plus souvent recouru, concernant les atteintes à de telles informations, à l'article 80.3°

qui la dispensait de leur attribuer une qualification secrète (cf. supra). Mais le concept même de secret technologique ou de secret économique dépasse les informations gouvernementales à objet économique ou industriel. Il couvre surtout des informations détenues par des personnes privées et pouvant intéresser la réussite économique ou technologique du pays. On peut donc se demander jusqu'où le secret de la défense nationale peut couvrir ces secrets technologiques et économiques, que les législateurs successifs ont, semble-t-il, voulu intégrer dans son champ d'intervention.

Comme nous l'avons vu (cf. supra), l'article 78 issu de la réforme du Code pénal de 1939 mentionnait déjà explicitement dans son premier alinéa les renseignements *« économiques ou industriels »* et énumérait parmi les supports du secret les *« matériels »* et les *« plans »*, de manière à couvrir certains types d'équipements et de documents techniques. Cette volonté du législateur de prendre en compte les nouveaux risques d'espionnage industriel qui apparaissaient dans l'entre-deux-guerres se traduisait aussi par l'adoption, peu de mois avant, du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre. Et, elle était, surtout, complétée par les dispositions de l'alinéa 3° de l'article 81 qui sanctionnaient lourdement quiconque *« sans autorisation préalable de l'autorité compétente, livrera ou communiquera à une personne agissant pour le compte d'une puissance ou d'une entreprise étrangère, soit une invention intéressant la défense nationale, soit des renseignements, études ou procédés de fabrication se rapportant à une invention de ce genre, ou à une application industrielle intéressant la défense nationale »*.

Ce dernier texte était fort important dans la mesure où il mentionnait *« une entreprise étrangère »*, mettant sur un pied d'égalité les actes d'espionnage industriel commis directement par un État étranger et ceux commis par une firme étrangère, que ce soit pour son propre compte ou indirectement pour le compte de son État d'origine [2]. Mais cet article consacrait aussi la nouvelle notion d'*« invention intéressant la défense nationale »*, qui permettait à l'État de se réserver le bénéfice des inventions intéressant la défense nationale et lui permit de mettre en place – par le décret-loi du 29 novembre 1939 – une procédure d'examen par le ministre de la défense des demandes de brevet (cf. infra).

La réforme de 1960 voulut confirmer, en apparence, cette prise en compte des secrets économiques et industriels. Certes, nous l'avons vu, l'abandon de tout effort de définition du secret de défense entraîna la disparition de la mention du caractère économique ou industriel des renseignements secrets. Mais, en revanche apparaissait désormais le terme *« procédé »* qui désigne clairement comme objet de protection des éléments techniques immatériels (savoir-faire ou inventions brevetables). Par ailleurs,

---

[2] On connaît, dès avant la seconde guerre mondiale, plusieurs cas d'espionnage économique et industriel perpétrés par des entreprises étrangères : Alfred Krupp, par exemple, fit en 1838 un voyage à Sheffield afin d'aller surprendre les secrets de fabrication de l'acier anglais (cf. Peter Batty, *La dynastie des Krupp*, R. Laffont). Cf. aussi, Oscar Ray, *Histoire de l'espionnage*, Gallimard, 1936, p. 241 à 248. Et le colonel Nicolaï, ancien chef du renseignement allemand durant la 1re guerre mondiale, écrivait en 1932 que l'organisation du renseignement *« connaît de tout ce qui, en fin de compte, peut donner la victoire sur l'ennemi, des affaires, du commerce, de l'industrie, de la politique, des armes. Son occupation n'est plus la recherche passive du renseignement. Elle prend une part, très active même, à la lutte économique et à la propagande extérieure et intérieure »* (Colonel Nicolaï, *Forces secrètes*, Editions de la nouvelle revue critique, 1932, p. 20).

l'article 77 modifié reprenait intégralement la rédaction de l'article 81.3° et la mise à jour de la législation sur les brevets d'invention maintint les pratiques antérieures d'examen préalable et de mise au secret.

Mais, pour autant, la réforme de 1960 n'a pas réussi en pratique à élargir véritablement le champ d'application du secret de défense au-delà de ses domaines de prédilection traditionnels. Faisant ainsi une synthèse rétrospective de la situation postérieure à 1960, le rapporteur de l'Assemblée nationale sur le projet de nouveau code pénal dut donc en rester à une conception classique en estimant que le secret de défense couvrait

> *« les renseignements économiques ou industriels, mais seulement dans la mesure où ils intéressaient la défense nationale. La protection contre l'espionnage s'arrête aux limites du " complexe militaro-industriel ", sous réserve de la loi du 26 juillet 1968. C'est pourquoi la commission de révision du Code pénal a considéré qu'il fallait à l'avenir assurer la protection des secrets mettant en cause les intérêts fondamentaux de la Nation, dont la défense n'est qu'un des éléments. »* [3]

Avant donc d'analyser en quoi la protection des intérêts fondamentaux de la nation peut contribuer à celle des secrets économiques et technologiques, il faut préciser que la protection des secrets technologiques et économiques intéressant la défense prend, traditionnellement, deux formes : d'une part, la protection du secret et le contrôle des armements et des matériels de guerre; d'autre part, l'application de certaines réglementations sans rapport direct avec la protection du secret mais qui assurent indirectement une certaine protection « périphérique » des secrets économiques et technologiques.

La protection du secret et le contrôle des inventions

Les informations relatives aux armements sont largement protégées par le secret de défense. Les *« documents relatifs à la conception, l'étude, la réalisation, l'affectation des matériels de guerre et équipements assimilés et à leur emploi »* appartiennent, en effet, à une des catégories de documents relevant du ministère de la défense exclus de la communication des documents administratifs [4]. De plus, de nombreux éléments témoignent du respect traditionnel du secret des armements. Cela ressort de la jurisprudence des tribunaux qui ont dès la fin du XIX^{e} siècle étendu leur répression aux armes de guerre et aux renseignements techniques les concernant. Mais cela ressort aussi des textes : ainsi l'article 12 du décret-loi du 18 avril 1939 qui impose l'obligation d'une autorisation préalable à toute exportation d'armes, précise que cette obligation ne fait pas obstacle à l'application des dispositions relatives à la *« répression de l'espionnage »*. Dans un autre domaine, l'ancien article 418 du Code pénal qui réprimait la violation du *« secret de fabrique »* (cf. infra sur cette

---

[3] *Rapport sur le projet de loi portant réforme des dispositions du Code pénal relatives à la répression des crimes et délits contre la Nation, l'État et la paix publique*, par M. François Colcombet, Tome I, *Assemblée nationale*, neuvième législature, séance du 26 septembre 1991, document n° 2244, p. 48.

[4] Cf. Ministère de la défense, arrêté du 17 novembre 1980, application de l'article 6 de la loi du 17 juillet 1978 portant diverses mesures d'amélioration entre l'administration et le public, *JORF* du 13 décembre 1980, p. 10924.

notion pénale réprimait la violation de certains secrets industriels) précisait que le maximum des peines prévues, *« sera nécessairement appliqué s'il s'agit de secrets de fabrique d'armes et munitions de guerre appartenant à l'État »*.

Ce secret des armements – qui ne couvre cependant jamais tous les armements, mais seulement ceux qui possèdent un caractère suffisamment innovant et peu connu [5] – s'étend, en France, à celui des exportations des matériels de guerre [6].

Ce secret des ventes d'armes est régulièrement critiqué, au motif qu'il servirait principalement à empêcher un contrôle démocratique des options économiques, politiques et militaires qui sous-tendent ces exportations [7]. Mais il demeure toujours invoqué par tous les gouvernements : on a constaté ainsi son utilisation, face à la justice, dans l'affaire Luchaire (sur cette affaire, cf. infra, chapitre 10). Mais ce secret sur les armements est aussi à l'origine de celui – plus large – qui couvre, en amont des matériels eux-mêmes, les *« inventions intéressant la défense nationale »* (selon l'expression employée par l'ancien article 77 et par l'instruction ministérielle du 13 février 1973 [8]).

Le régime des inventions intéressant la défense nationale

Ce n'est qu'en 1916 qu'une loi prescrivit les premières mesures relatives aux brevets d'invention susceptibles de couvrir des matériels d'armement. [9]

Dans l'intervalle, il demeurait possible à l'inventeur d'un dispositif susceptible d'intéresser la défense nationale (et dont la divulgation devenait, de ce fait, assimilable à un acte de trahison) de se faire attribuer – sans aucune précaution particulière – un brevet (dont la publication risquait de retirer tout caractère secret à l'invention considérée) [10]. Il en fut ainsi dans une affaire célèbre, qui défraya la chronique entre 1885 et

---

[5] Déjà, à la fin du siècle dernier, l'auteur d'un ouvrage sur l'espionnage, tournait en dérision le secret abusif invoqué à propos d'un modèle très courant de fusil (Lieutenant A. Froment, *L'espionnage militaire – Les fonds secrets de la guerre et le service des renseignements en France et à l'étranger*, Éditions F. Juven, Paris, 1897, p. 133).

[6] Une circulaire du 8 février 1974, signée du ministre de la défense de l'époque, M. Robert Galley, préciserait notamment *« que tout ce qui touche à la vente de matériels d'armement français doit être considéré comme rigoureusement secret et qu'aucune information ne peut être communiquée à leur sujet »* [extrait cité in Eric Gerdan, *A... comme armes*, Alain Moreau, 1975 (coll. dossiers poche), p. 14].

[7] Cf., par exemple, André Postel-Vinay, « Renoncer au secret », *Le Monde*, 2 juillet 1991.

[8] Instruction interministérielle n° 9062/DN/CAB relative aux inventions intéressant la défense nationale du 13 février 1973, *JORF*, 25 février 1973, p. 2109.

[9] Loi du 12 avril 1916 relative aux inventions intéressant la défense nationale, *JORF*, 14 avril 1916, p. 3140. Sur ce texte et sur l'évolution de la législation française en la matière, cf. Nathalie Wuylens, *Défense nationale et propriété industrielle*, Thèse, Paris II, 1998, p. 37 et p. 87 et s.

[10] Dans son manuel de droit industriel, Pelletier – avocat et professeur de propriété industrielle au CNAM – pouvait écrire en 1893 : *« nous pensons (...) que l'expropriation pour cause d'utilité publique n'est pas, dans l'état actuel de notre législation, applicable à la propriété des brevets. Nous croyons devoir ajouter, toutefois, que, selon nous, il y aurait peut-être quelque réforme à apporter sur ce point à notre législation, dans le but d'apporter à l'État les moyens de se réserver l'exploitation exclusive du brevet, dans le cas exceptionnel où l'intérêt de la défense nationale l'exigerait »* (Michel Pelletier, *Droit industriel – Brevets d'invention, marques de fabrique, modèles et dessins, nom commercial, concurrence déloyale*, Paris, Librairie Polytechnique, 1893, p. 64).

1891, relative à l'invention d'un nouvel explosif pour l'artillerie dénommé la mélinite [11].

Mais la loi de 1916, qui prévoyait la possibilité pour l'État de prendre connaissance des demandes de brevet, d'en interdire éventuellement la divulgation et d'exproprier celles qui intéressaient la défense nationale, n'avait été prise que pour la durée de la guerre et cessa de produire ses effets en décembre 1919.

Elle ne fut suivie que par un décret-loi du 30 octobre 1935 qui créa la possibilité pour l'État d'exproprier les inventions – brevetée ou non – intéressant la défense nationale. Jugée insuffisante dans ses modalités (puisque, notamment, les inventeurs demeuraient libres de divulguer leur invention ou leur brevet tant que l'État ne leur avait notifié l'ouverture de la procédure d'expropriation), cette procédure fut à son tour complétée en 1939, par le nouvel article 81 alinéa 3 du code pénal [12] et, d'autre part, par le décret du 29 novembre 1939 qui élargissait les prérogatives gouvernementales à l'ensemble des inventions intéressant la défense (et non plus, simplement, aux brevets d'invention), qui disjoignait la mise au secret de l'invention de l'expropriation et qui instaurait un délai de huit mois durant lequel aucune demande de brevet, quel que soit son objet, ne pouvait être publiée, afin que le ministre de la défense puisse en prendre connaissance dans l'intervalle [13].

L'application de ce dernier décret – pris, lui aussi, pour la durée des hostilités – fut prorogée à plusieurs reprises après la fin de la Seconde guerre mondiale, jusqu'à ce que la loi du 2 janvier 1968 sur les brevets d'invention n'en reprenne – avec quelques modifications – l'essentiel des dispositions. Celles-ci figurent désormais dans le Code de la Propriété intellectuelle et les textes réglementaires qui y sont associés.

L'examen préalable par le ministère de la défense

Concernant l'examen préalable par le ministre de la défense, l'article L. 612-8 du Code de la propriété intellectuelle prévoit que *« le ministre chargé de la défense est habilité à prendre connaissance auprès de l'Institut national de la propriété industrielle, à titre confidentiel, des demandes de brevets »*.

---

[11] L'inventeur du procédé originel, Eugène Turpin, bien qu'ayant contacté les Armées, prit un brevet en 1885 qui lui fut rapidement délivré et à propos duquel le ministère de la Guerre ne négocia qu'une cession de droit d'exploitation assortie d'une obligation de confidentialité de dix mois. Plusieurs années plus tard, Turpin, estimant que ses droits n'avaient pas été respectés, accepta d'effectuer certaines expériences en Grande-Bretagne et publia dans un ouvrage paru en 1891 quelques plans décrivant les obus et détonateurs mis au point pour utiliser la mélinite (cf. Eugène Turpin, *Comment on a vendu la mélinite*, Albert Savine éditeur, Paris, 1891). Il fut alors condamné pour divulgation de documents secrets (CA Paris, 16 juillet 1891 et 11 août 1891; Cass. Crim., 24 septembre 1891, reproduits *in* Mennevée, *op. cit.*, pp. 451-458).

[12] Cet article – introduit dans le Code pénal par le décret-loi du 29 juillet 1939 réprimait la livraison des *« inventions intéressant la défense nationale »* à des personnes *« agissant pour le compte d'une puissance ou d'une entreprise étrangère »*. Il fut repris, à l'identique, par l'article 77 du Code pénal en 1960.

[13] Décret du 29 novembre 1939 relatif aux inventions intéressant la défense nationale, *JORF*, 10 décembre 1939. Sur l'historique de ces textes, cf. J.-P. Palewski, « Les inventions concernant la défense nationale », *Etudes sur la propriété industrielle, littéraire et artistique – Mélanges Plaisant*, Sirey, 1959, pp. 119 et s.

Cet article, est complété, d'une part, par les dispositions réglementaires des articles R. 612-26 CPI à R. 612-32 CPI [14], et d'autre part – comme auparavant – par trois dispositions législatives identiques concernant les demandes de brevets européens (art. L. 614-3 CPI), les demandes internationales (art. L. 614-19 CPI), ainsi que les demandes de certificats d'obtention végétale (art. L. 623-8 CPI) [15].

Ces quatre articles législatifs établissent pour les demandes déposées auprès de l'INPI ou du comité de la protection des obtentions végétales une procédure d'examen préalable qui constitue, en réalité, une véritable suspension temporaire des droits du titulaire [16].

En effet, tant que le ministre chargé de la propriété industrielle n'a pas donné – sur avis du ministre de la défense – son autorisation, la procédure de propriété industrielle est suspendue ainsi que toute publication ou exploitation par le titulaire [17].

Pour procéder à leur examen technique et décider s'il y a lieu d'accorder ou non l'autorisation de libre exploitation et de divulgation, les services du ministère de la défense [18] disposent d'un délai maximal fixé par la loi [19]. S'ils estiment que le contenu de la demande nécessite que l'invention ou l'obtention végétale concernée doit demeurer confidentielle, ils peuvent faire proroger – par une décision du ministre chargé de la propriété industrielle – ces différentes interdictions de divulguer ou d'exploiter pour une durée d'un an renouvelable (articles L. 612-10 CPI, L. 614-5 CPI, L. 614-21 CPI). À l'inverse (et c'est le cas le plus fréquent), il est possible, à tout moment dans le même délai, de donner un avis favorable à la divulgation et à l'exploitation. Et pour prémunir le titulaire contre l'éventuel silence de l'administration, si aucune autorisation ou réquisition n'a été prononcée dans le délai de cinq mois, l'autorisation est considérée comme *« acquise de plein droit »*.

Dans la pratique, on observe que le délai de rétention d'un brevet est en moyenne de quinze jours pour les inventions n'intéressant manifeste-

---

[14] Ces articles, codifiés dans le Code de la propriété intellectuelle, sont issus du Chapitre II du décret n° 79-822 du 19 septembre 1979 relatif aux demandes de brevet d'invention et de certificats d'utilité, à la délivrance et au maintien en vigueur de ces titres.

[15] Concernant les certificats d'obtention végétale, le Code prévoit – comme précédemment – que cette procédure d'examen préalable ne porte que sur une liste d'espèces (art. L. 623-9 CPI) arrêtée conjointement par les ministres de la défense et de l'agriculture. En revanche, l'on remarquera que les dispositions relatives à la protection des topographies de semi-conducteurs ne prévoient pas ce contrôle alors que l'on connaît l'importance des composants électroniques (et notamment des circuits spécifiques) pour les matériels de défense.

[16] Pour une présentation récente du régime d'examen préalable par la défense nationale, cf. l'intervention de Martine Hiance in *La propriété industrielle et le secret* – Centre Paul Roubier, journée d'étude du 4 avril 1995, Litec, 1996, pp. 36-39.

[17] Cf. les articles L. 612-9, L. 614-4, L. 614-20 CPI (pour les brevets) et L. 623-9 CPI pour les obtentions végétales.

[18] Il s'agit du bureau de la propriété industrielle (BPI, actuellement rattaché à la Direction des systèmes de forces et de la prospective de la DGA) qui procède à un premier tri, puis – pour les demandes de brevet qui paraissent intéressantes – des experts appartenant aux différents services techniques compétents de la DGA (cf. Jacques Cochet-Grasset, « Les inventions et la défense », *Armées d'aujourd'hui*, mars 1978, p. 16 et N. Wuylens, *op. cit.*, pp. 97-109).

[19] Ce délai est de cinq mois à dater du jour du dépôt de la demande de brevet français (article L. 612-9, alinéa 2). En revanche, pour les demandes de brevet européen, le délai est de quatre mois ou – lorsque cette demande invoque une priorité française – de quatorze mois à dater de la date de priorité (article L. 614-4, dernier alinéa). Pour les demandes internationales,

ment pas la défense et de trois mois pour celles nécessitant un examen plus poussé [20] et que la mise au secret totale ne représente en définitive que quelques demandes brevets pour mille [21]. La grande majorité concerne, d'ailleurs, des inventions déjà connues par le ministère de la défense car réalisées dans le cadre de marchés classés [22].

L'obligation partielle du premier dépôt de brevet en France

L'une des conséquences juridiques importantes de ces dispositions sur le contrôle et le secret des brevets (ou des obtentions végétales) intéressant la défense nationale, concerne – pour des raisons pratiques évidentes – le lieu de premier dépôt.

Dès lors, en effet, qu'un inventeur a déjà réalisé un premier dépôt à l'étranger, il n'est plus possible à l'administration française de prétendre ultérieurement mettre au secret une demande de brevet français portant sur la même invention. En toute rigueur, les textes législatifs sur les brevets et l'actuel Code de la propriété intellectuelle devraient donc imposer que toutes les demandes de brevet formulées par des résidents français soient obligatoirement déposées en premier en France, avant de pouvoir – à l'expiration du délai d'examen par la DGA – faire l'objet d'extensions à l'étranger [23].

Cette logique a prévalu concernant le dépôt des demandes de brevet européen et international, pour lesquelles le code dispose que *« la demande doit être déposée auprès de l'Institut national de la propriété industrielle, lorsque le déposant a son domicile ou son siège en France et qu'il ne revendique pas la priorité d'un dépôt antérieur en France. »* [24]

Mais elle n'existe pas sous cette forme générale en ce qui concerne les demandes de brevets français et de certificats d'obtention végétale. Concernant ces titres, les seules interdictions relatives au transfert et à l'exploitation hors des frontières résultent des textes du Code pénal ou issus de lui.

---

le délai est de cinq mois, ou de treize mois à dater de l'éventuelle date de priorité (article L. 614-20, dernier alinéa).

[20] Cf. Marie-Angèle Perot-Morel, « Défense nationale et brevet d'invention », *Ares - Défense et Sécurité*, 1981, p. 164.

[21] Cf. Jean Foyer et Michel Vivant, *Le droit des brevets*, PUF, 1991, p. 282. Dans le même sens, L'IGA Cochet-Grasset et M^me^ Carpentier de l'INPI signalaient que les brevets mis au secret n'étaient qu'*« environ 150 par an sur un total de 30.000 brevets déposés »* et qu'il y avait, à cette date, *« 1.000 brevets au secret, les plus anciens datant de 1949 »* (*Actes des journées Science et Défense*, Palaiseau, 26 et 27 avril 1983, p. 104). Plus récemment, M^me^ Martine Hiance, directeur général adjoint de l'INPI, recensait 34 dépôts secrets effectués en 1994 et 1.600 prorogations annuelles de la période de mise au secret (cf. son intervention, *in* journée d'étude du Centre Paul-Roubier, *op. cit.*, pp. 37-38). M^me^ Wuylens signale, pour sa part, dans sa thèse le chiffre de 1.400 demandes classifiées et une baisse régulière du taux de mise au secret (N. Wuylens, *op. cit.*, p. 129).

[22] Cf. M. Hiance, *op. cit.*, p. 37; J. Cochet-Grasset, « Le Bureau des Brevets et Inventions », *Bulletin d'information et de liaison, l'Armement*, 1979, n° 57, p. 17; M.-A. Perot-Morel, *op. cit.*, p. 164. Sur la notion de marché classé de défense, cf. infra.

[23] Cf. l'intervention, en ce sens, de Michel Moncheny, conseil en propriété industrielle, à la journée d'étude du Centre Paul-Roubier, *op. cit.*, p. 47.

[24] Article L. 614-2 CPI, alinéa 2 (pour les demandes de brevet européen) et article L. 614-18 CPI (pour les demandes de brevet international).

Sous l'empire des textes en vigueur depuis 1939, le Code pénal interdisait explicitement la transmission *« sans autorisation préalable »* à une puissance ou une entreprise étrangère d'une *« invention intéressant la défense nationale »* (art 81.3°, puis 77, cf. supra), ce qui couvrait notamment – d'après l'instruction interministérielle du 13 février 1973 – le cas des premiers dépôts à l'étranger d'un brevet se rapportant à une telle invention [25].

Dès lors, jusqu'en 1994 l'obligation d'un premier dépôt en France était limitée aux seules demandes nationales concernant les inventions intéressant la défense, alors qu'elle était générale en matière de demandes européennes ou internationales.

À cette situation déjà complexe, l'entrée en vigueur du nouveau Code pénal a introduit un élément perturbateur supplémentaire, puisque désormais – comme nous l'avons vu –, la notion d'*« invention intéressant la défense nationale »* a disparu au profit d'infractions relatives soit au secret de défense lui-même, soit à la livraison d'informations dont la divulgation porterait atteinte aux intérêts fondamentaux de la nation. Peut-on considérer que ces différentes dispositions pénales suffisent à interdire la sortie du territoire de toute information relative à une invention faite en France et non encore brevetée ? À l'évidence, ce n'est pas le cas : seules les inventions brevetables présentant un intérêt au regard des intérêts fondamentaux de la nation sont soumises à une restriction de sortie [26].

De plus, si l'on se place du point de vue de la protection du secret de défense *stricto sensu,* la définition donnée par l'article 413-9 et fondée sur le critère des mesures de protection (cf. supra, chapitre 6) a pour conséquence qu'outre les demandes de brevet mises au secret après leur dépôt, le secret de défense ne peut couvrir que des informations relatives à des inventions qui auraient fait l'objet, lors de leur conception, de mesures de protection du secret (c'est-à-dire qu'il ne peut s'agir que d'inventions non encore brevetées ayant été conçues dans le cadre, par exemple, d'un marché classé de défense ou à l'intérieur d'un établissement public travaillant pour le compte de la défense).

Dans ces conditions, les nouvelles dispositions du Code pénal ne changent pas fondamentalement la situation : en ce qui concerne les demandes de brevet français et de certificat d'obtention végétale, il n'existe toujours pas d'obligation générale d'un premier dépôt en France s'imposant aux résidents français. Cette obligation n'existe qu'indirectement pour les inventions ou obtentions végétales dont la conception a été entourée de mesures spéciales de protection (et qui, donc, sont susceptibles de constituer des secrets de défense) ainsi que pour celles (moins aisées à identifier) qui pourraient être considérées comme sensibles au regard des intérêts fondamentaux de la nation. S'il y a donc là un élargissement possible des cas où le premier dépôt devra être effectué en France pour

---

[25] *« Sauf cas exceptionnels, aucune autorisation de dépôt à l'étranger d'une demande de brevet ou certificat d'addition couvrant une invention intéressant la défense nationale n'est accordée avant le dépôt initial en France de la demande de brevet, certificat d'utilité ou certificat d'addition couvrant cette invention »* (Instruction n° 9062, précitée).

[26] *« Le législateur n'a pas jugé utile de sanctionner pénalement la transmission à l'étranger de données sans caractère stratégique »* (M. Hiance, *op. cit.*, p. 48).

éviter tout risque d'infraction pénale, force est de constater que le nouveau code pénal n'impose aucunement une généralisation de l'obligation en question.

Mais la disparition de l'ancien article 77 et de l'interdiction d'exportation qu'il édictait a accru le trouble et l'insécurité juridique pour les entreprises. Jusqu'alors, en effet, les entreprises souhaitant déposer à l'étranger une première demande de brevet pour une invention dans un domaine susceptible d'intéresser la défense (par exemple, dans un domaine à double usage) pouvaient consulter au préalable le ministère de la défense et obtenir, le cas échéant, une autorisation pour ce faire. Aujourd'hui, ce recours auprès de l'administration n'est plus possible car l'infraction en cause ne concerne plus seulement la défense mais l'ensemble des intérêts fondamentaux de la nation. Le ministère de la défense ne se sent donc plus en mesure de porter une appréciation sur les demandes qui lui sont soumises et de délivrer, éventuellement, une autorisation. Et comme aucune administration (y compris le SGDN) ne se reconnaît actuellement compétente pour formuler un avis *a priori* sur la possibilité d'atteintes aux intérêts fondamentaux de la nation, tout dépôt à l'étranger d'une première demande de brevet par une entreprise française ou concernant une invention faite en France est à la fois administrativement libre et pénalement potentiellement répréhensible.

C'est pour sortir de cette situation inconfortable que le Conseil supérieur de la propriété industrielle a engagé en 1999 l'étude d'une future réforme des dispositions légales et réglementaires relatives aux inventions intéressant la défense nationale. Sans préjuger des propositions finales du gouvernement sur ce dossier, il paraîtrait nécessaire soit de recréer une disposition pénale similaire à l'ancien article 77 du Code pénal, soit au moins d'imposer un premier dépôt en France pour les inventions intéressant la défense nationale.

Le régime juridique des demandes mises au secret

Concernant le régime juridique s'appliquant aux demandes de brevet ou de certificats d'obtention végétale dans la période initiale de leur examen ou dans la période de prorogation éventuelle des mesures de secret, nous nous trouvons face à une situation qui se caractérise par trois éléments :

– suspension de la procédure de traitement de la demande par les organismes de propriété industrielle ;

– interdiction d'exploitation par l'inventeur ;

– secret de l'invention et de la demande de brevet correspondante [27] ou de la demande de certificat d'obtention végétale.

Le non-respect des deux dernières contraintes qui s'imposent au titulaire ainsi qu'à tous les tiers [28] est sanctionné – dès lors qu'il est

---

[27] Ce secret s'attache au contenu même de l'invention, de sorte que la renonciation du titulaire ou la déchéance du titre de propriété industrielle ne fait pas disparaître l'interdiction de divulgation et d'exploitation (cf. J. Cochet-Grasset, « Brevets d'invention - Défense nationale », *Jurisclasseur Brevets*, fascicule 300, août 1981, p. 4).

[28] Il a été, notamment, jugé par la Cour de cassation que constituait une violation de l'interdiction de divulgation de l'invention, le fait de faire procéder à une saisie contrefaçon à

volontaire – par des peines spécifiques prévues par le Code de la propriété intellectuelle (articles 615-13 pour les demandes de brevets français, 615-15 pour les demandes internationales, 615-6 pour les demandes européennes et 623-35) :

– une peine d'amende (3.000 F à 30.000 F pour les demandes de brevet français et de certificat d'obtention végétale, 3.000 F à 40.000 F pour les demandes européennes ou internationales);

– une peine d'emprisonnement complémentaire de un à cinq ans *« si la violation a porté préjudice à la défense nationale. »*

Mais à ces sanctions peuvent s'en ajouter d'autres – plus lourdes – provenant du Code pénal. L'ancien article 77 du Code pénal n'ayant pas actuellement de successeur direct dans le nouveau Code pénal, l'interprétation officielle se contente de considérer que son objet est aujourd'hui couvert par la définition large du nouvel article 411-6 nCP[29]. Il est effectivement probable que la divulgation d'une invention mise au secret à une puissance ou organisation étrangère (cas prévu par l'ancien article 77) serait de nature à porter atteinte aux intérêts fondamentaux de la nation, et particulièrement à celui qui s'attache à la préservation du potentiel *« scientifique et économique »* national.

Mais on peut penser que, désormais, les nouvelles dispositions réprimant la compromission d'un secret de défense (articles 413-10 nCP et 413-11 nCP) pourraient être également sollicitées dans certains cas de divulgation d'inventions mises au secret. En effet, la nouvelle définition du secret de défense posée par l'article 413-9 nCP permet de considérer qu'une demande de brevet d'invention conservée au secret sur avis du ministre de la défense fait partie des *« renseignements, procédés (...) qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion »* (en l'occurrence, l'interdiction de divulgation et d'exploitation) et *« dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale ».*

Le niveau de la sanction punissant une divulgation non autorisée de l'invention mise au secret dépendra donc de l'existence d'une éventuelle atteinte aux intérêts fondamentaux de la nation et d'une possible transmission à l'étranger.

Les conditions d'exploitation d'une invention mise au secret

La première règle applicable en cas de prolongation des interdictions de divulgation et d'exploitation consiste en une juste indemnisation du préjudice subi par le titulaire en raison de cette interdiction. Une telle

---

l'encontre du breveté avant que celui-ci n'ait reçu l'autorisation de divulgation et d'exploitation de sa demande de brevet (Cass. Com., 4 octobre 1971, Bull. Civ. 1971 n° 222, *PIBD*, 1972, p. 68; cf. également, N. Wuylens, *op. cit.*, p. 113).

[29] Cf. dans ce sens, ministère de la Justice, Circulaire du 14 mai 1993 présentant les dispositions du nouveau Code pénal et de la loi n° 92-1336 relative à son entrée en vigueur, *JORF*, octobre 1993, p. 225; *Rapport sur le projet de loi portant réforme des dispositions du Code pénal relatives à la répression des crimes et délits contre la Nation, l'État et la paix publique*, par M. François Colcombet, Tome I, *Assemblée nationale*, neuvième législature, séance du 26 septembre 1991, document n° 2244, p. 49.

indemnisation est prévue – en matière de brevet – par le second alinéa de l'article L. 612-10 aux termes duquel :

> *« La prorogation des interdictions édictées en vertu du présent article ouvre droit à une indemnité au profit du titulaire de la demande de brevet, dans la mesure du préjudice subi. »*

Une disposition identique est reprise par l'article L. 623-10 concernant les obtentions végétales. En ce qui concerne les seules demandes de brevets, l'article L. 612-10 prévoit également qu'en cas de litige sur le montant de l'indemnité compensatoire [30], toutes les étapes du litige judiciaire à ce sujet doivent être jugées en *« chambre du conseil »* afin de garantir la confidentialité des débats et qu'ils ne soient pas l'occasion d'une violation involontaire du secret de défense.

Ces mesures destinées à sauvegarder le secret dans le règlement du litige pécuniaire entre l'État et le titulaire sont complétées par celles de l'article R. 612-30 CPI, selon lesquelles les décisions rendues en cette matière par la juridiction *« ne contiennent aucune analyse de l'invention de nature à en entraîner la divulgation. Seuls le ministère public, les parties ou leurs mandataires peuvent obtenir copie des décisions rendues. Si une expertise est ordonnée, elle ne peut être effectuée que par des personnes habilitées par le ministre de la défense ».*

Le préjudice en question ayant tendance à s'aggraver proportionnellement à la durée de la prorogation de l'interdiction, l'article L. 612-10 prévoit la possibilité de demander une révision de l'indemnité après un délai d'un an au-delà de la date du jugement définitif fixant le montant de l'indemnité.

À l'inverse de l'indemnisation du titulaire, aucune disposition légale ou réglementaire ne préserve les droits des tiers pouvant avoir à souffrir d'une éventuelle mise au secret, comme par exemple ceux d'un tiers empêché d'exercer une action en revendication contre une demande de brevet mise au secret [31]. Mais cette hypothèse demeure très exceptionnelle, ce qui justifie sans doute l'absence d'une disposition légale protégeant les tiers dans ce type de cas [32].

Dans le même but de limiter le préjudice subi par le titulaire de la demande de brevet mise au secret, il existe la possibilité d'une extension à l'étranger de la demande de brevet dans d'autres pays alliés. La France a, notamment, signé et mis en œuvre en 1965 un accord OTAN du 21 septembre 1960 consacré à *« la sauvegarde mutuelle du secret des inventions intéressant la défense et ayant fait l'objet de demandes de brevet. »* [33] Les considérants de cet accord résument bien son objet :

> *« Considérant que la limitation territoriale du champ de protection des inventions qui résulte de cette interdiction* [de divulgation] *peut nuire*

---

[30] Jurisprudence sur le montant et l'assiette de l'indemnité : Cass. Com., 5 janvier 1963; Cass. Com., 18 mars 1968; CA Paris, 20 janvier 1971, *PIBD*, 1971.III.206 (interdiction de dépôt à l'étranger et perte du droit de priorité unioniste, préjudice moral).

[31] Comme ce fut le cas dans l'affaire Blanchard c./ Grunler, évoquée plus haut.

[32] M.-A. Perot-Morel, *op. cit.*, p. 171.

[33] Cf. décret n° 65-234 du 26 mars 1965 portant publication de l'accord OTAN pour la sauvegarde mutuelle du secret des inventions intéressant la défense et ayant fait l'objet de demandes de brevet du 21 septembre 1960, *JORF*, 1er avril 1965, p. 2565.

aux demandeurs de brevets et, par suite, à la collaboration économique entre les pays de l'Organisation du traité de l'Atlantique Nord; (...) Considérant que, si le gouvernement dont émane l'interdiction est disposé à autoriser le dépôt d'une demande de brevet dans un ou plusieurs autres pays de l'Organisation du traité de l'Atlantique Nord, pour autant que les gouvernements de ces pays mettent également l'invention au secret, ces gouvernements ne sauraient refuser la mise au secret... ».

Au titre de cet accord, les titulaires d'une demande de brevet mise au secret sur décision du Gouvernement français peuvent effectuer – par l'intermédiaire de la voie diplomatique (courrier diplomatique protégé) – une demande de dépôt de cette même invention dans un autre pays de l'OTAN, lequel a l'obligation de la mettre également au secret et de lui attribuer une classification de sécurité d'un niveau au moins égal à celui de la classification de sécurité définie par les services français. Ce faisant, le titulaire – tout en ne pouvant pas retrouver à l'étranger la liberté de divulgation et d'exploitation qui lui a été refusée en France – peut se garantir contre une éventuelle contrefaçon qui serait exécutée dans un autre pays de l'OTAN et se constituer une antériorité dans ce pays qu'il sera à même d'invoquer à l'expiration du délai de mise au secret.

De la même façon, la France a conclu plusieurs accords bilatéraux ayant la même finalité, notamment avec les États-Unis [34], l'Allemagne [35] et la Suède. [36]

Signalons, pour être complet, que dans l'intérêt de la défense nationale, peuvent être également prises deux autres mesures autoritaires concernant des brevets : l'attribution d'une licence d'office (article L. 613-19 CPI) et l'expropriation (article L. 613-20 CPI). Ces deux procédures ont pour but de permettre l'exploitation directe par l'État, ou par certains de ses sous-traitants auxquels il en confierait la tâche, d'un brevet pouvant être utile à la défense. Mais en tant que telles, ces mesures ne sont pas propres aux seuls brevets mis au secret au titre des procédures décrites précédemment. Elles peuvent tout à fait frapper une invention ayant déjà fait l'objet d'une autorisation de divulgation et d'exploitation [37].

Le contrôle des exportations d'armement

La réglementation française des matériels de guerre prévoit que toute activité industrielle ou commerciale relative à ces matériels est soumise

---

[34] Échange de lettres entre la France et les États-Unis d'Amérique au sujet de la procédure pour le dépôt réciproque, en France et aux États-Unis d'Amérique, des demandes de brevets conservées secrètes des 28 mai et 10 juillet 1959 (publié par le décret n° 62-223 du 27 février 1962).

[35] Accord entre le gouvernement de la République française et le gouvernement de la République fédérale d'Allemagne pour la sauvegarde mutuelle du secret des inventions et des informations techniques intéressant la défense, signé le 28 septembre 1961 (publié par le décret n° 62-102 du 25 janvier 1962, *JORF*, 1er février 1962, p. 1086).

[36] Accord entre le gouvernement de la République française et le gouvernement du Royaume de Suède pour la sauvegarde mutuelle du secret des inventions intéressant la défense et ayant fait l'objet de demandes de brevet du 15 mars 1984 (publié par le décret n° 84-488 du 19 juin 1984, erratum du 17 mai 1988).

[37] Sur le régime et les modalités de la licence d'office et de l'expropriation, cf. notamment, Nathalie Wuylens, *Les mesures autoritaires de l'État pour les besoins de la défense nationale*,

à autorisation préalable. Dès lors, les exportations en sont interdites sauf dérogation gouvernementale accordée discrétionnairement par le Premier ministre. Ces principes ont été fixés par le décret-loi du 18 avril 1939. Ce texte – toujours en vigueur – établit une liste en huit catégories des types de matériels considérés comme *« matériels de guerre, armes et munitions »* [38] et dispose que la fabrication et le commerce de tels produits *« ne peut s'exercer qu'après autorisation de l'État et sous son contrôle. »*

Ce contrôle de l'État porte à la fois sur la nationalité des capitaux et des dirigeants [39], sur les règles de protection du secret et de sécurité au sein de ces entreprises, sur la qualité technique des processus de production et des matériels produits ainsi que sur le prix de revient de ces matériels.

Le même décret-loi précise également que *« l'exportation sous un régime douanier quelconque, sans autorisation, des matériels de guerre et matériels assimilés est prohibée »* et qu'*« il ne devra être accepté aucune commande en vue de l'exportation des matériels (...) sans agrément préalable donné dans des conditions fixées par arrêté interministériel. Il ne devra non plus, sans le même agrément, être procédé, aux fins de cession ou de livraison ultérieures à l'étranger, à aucune présentation ni à aucun essai de ceux de ces matériels, visés ci-dessus, qui seront définis par ledit arrêté. Il en sera de même pour la cession des licences commerciales de fabrication et de tous les documents nécessaires pour l'exécution des fabrications »*.

Les exportations d'armement (et les importations, qui suivent le même régime) à partir de la France constituent donc juridiquement des exceptions limitativement autorisées par le Gouvernement au principe général de non-exportation. Ces dérogations relèvent du pouvoir discrétionnaire de l'administration, et le Conseil d'État comme la Cour de Cassation leur refusent le caractère d'*« actes de gouvernement »* [40]. Ils restent dès lors soumis à un contrôle – restreint – du juge administratif et pourraient, dans certaines conditions, engager la responsabilité de l'administration [41].

Sur le plan de la procédure, différentes autorisations successives doivent être demandées et obtenues par l'exportateur : des agréments préalables pour les démonstrations, la remise d'offres, leur négociation,

---

mémoire de DESS de propriété industrielle, Université Paris II, 1992/1993, p. 31 et s.; M.-A. Perot-Morel, *op. cit.*, pp. 171 à 178; Catherine Blaizot-Hazard, *Les droits de propriété intellectuelle des personnes publiques en droit français*, LGDJ, 1991, pp. 121-125.

[38] La dernière version de cette liste résulte d'un décret du 6 mai 1995, *JORF*, 7 mai 1995, pp. 7458 et s.

[39] Les critères relatifs à la nationalité de l'entreprise et de ses dirigeants en matière de commerce et de fabrication des matériels de guerre sont fixés par l'article 7 du décret n° 73-364 du 12 mars 1973.

[40] Cf. notamment Cass. Civ. 1re, 30 juin 1992, *Association européenne Droit contre Raison d'État c. Avions Marcel Dassault - Breguet Aviation*, note David Ruzié, *Droit et Défense*, n° 93/2, p. 74.

[41] Cf. notamment CE Ass, 29 juin 1962, *Société Manufacture des machines du Haut Rhin* (Manurhin), Rec. 432, arrêt dans lequel le Conseil d'État a refusé de faire jouer, à propos d'un refus d'autorisation d'exportation d'armes de guerre, la responsabilité sans faute de l'administration du fait des actes légalement pris, en raison du fait que *« la société requérante ne pouvait ignorer l'aléa que comportait nécessairement la passation d'un tel contrat »* (dans le même sens – s'agissant non de matériel de guerre mais de technologie nucléaire civile à double usage, CE, *Robatel*, 19 février 1988, *A.J.D.A.*, 1988, p. 354 et s.). Une telle jurisprudence n'exclut pas toute possibilité de voir la responsabilité de l'État engagée à l'occasion d'une décision d'exportation de matériels de guerre, par exemple dans le cas où la décision en question serait entachée d'illégalité.

l'acceptation des commandes, les cessions de droits de propriété industrielle ou de données techniques, puis l'autorisation d'exportation elle-même (c'est-à-dire la dérogation à la prohibition de sortie) [42]. Et jusqu'à décembre 1999, la simple prospection était également soumise à agrément [43]. Ce système à plusieurs niveaux est propre à la France, la plupart des pays occidentaux ne connaissant qu'une seule procédure d'autorisation d'exportation. Une liste particulière regroupe en six catégories les matériels soumis à ces procédures de contrôle à l'exportation [44]. Elle est plus détaillée que celle citée plus haut qui concerne les matériels soumis à autorisation de fabrication et de commerce, et comprend notamment, en plus des matériels de guerre à proprement parler, certains produits à double usage comme les lanceurs spatiaux.

Les agréments préalables sont accordés au nom du Premier ministre par le Secrétariat général de la défense nationale (SGDN) après avis de la Commission interministérielle d'Étude des exportations de matériel de guerre (CIEEMG) [45]. Mais lorsque les agréments préalables ont été obtenus et le contrat conclu, l'industriel doit encore obtenir du ministère des Finances (Direction générale des douanes et des droits indirects) la délivrance d'une Autorisation d'exportation de matériel de guerre (AEMG) afin de pouvoir faire sortir du territoire les matériels objets du contrat.

La demande d'AEMG ainsi qu'une déclaration d'autorisation de sortie sont présentées par l'exportateur à la direction des relations internationales (D.R.I.) de la DGA, qui la vise puis la transmet successivement au Secrétariat général de la défense nationale ainsi qu'au Ministère des Affaires étrangères. Cette consultation écrite permet aux principaux ministères intéressés de vérifier que la demande d'exportation est effectuée en conformité avec les agréments précédemment obtenus après avis de la CIEEMG. Mais elle permet aussi d'exercer un dernier contrôle d'opportunité avant le départ définitif du matériel. Une fois que tous les ministères ont donné leur accord, la direction générale des douanes délivre l'AEMG à l'exportateur.

En complément de cette procédure de contrôle, deux éléments sont censés permettre aux autorités françaises de s'assurer de l'arrivée à destination et de la non-réexportation clandestine des matériels de guerre

---

[42] Cette procédure est actuellement définie par l'arrêté du Premier ministre du 2 octobre 1992, (*JORF*, 6 octobre 1992). Un récent rapport parlementaire en décrit avec beaucoup de précisions le déroulement (cf. Rapport d'information sur le contrôle des exportations d'armement, *Assemblée nationale,* document n° 2334, 25 avril 2000).

[43] Dès 1991, le Gouvernement avait envisagé – pour soutenir les industriels français de l'armement face à la concurrence – de supprimer l'agrément préalable de la phase de prospection. Mais la révélation de ce projet dans la presse (*Le Canard Enchaîné*, 10 avril 1991; *Le Monde*, 18 avril 1991), à quelques semaines de la fin des hostilités en Irak, avait fait renoncer le Gouvernement. Cet agrément a été finalement supprimé par l'arrêté du 20 décembre 1999 (*JORF* du 26 décembre 1999).

[44] La liste actuellement en vigueur a été fixée par l'arrêté du Premier ministre du 20 novembre 1991, *JORF*, 22 novembre 1991.

[45] Cette commission, créée en 1949 et modifiée en 1955 (décret n° 55-965 du 16 juillet 1955), regroupe mensuellement, sous la présidence du secrétaire général de la défense nationale, les représentants des ministères des Finances, des Affaires étrangères et de la Défense, auxquels s'ajoutent souvent d'autres administrations (Industrie, Intérieur et Coopération notamment). En pratique, les services de la Direction des relations internationales (DRI) de la Délégation générale pour l'Armement (DGA) assurent l'instruction préalable des dossiers soumis à la CIEEMG.

exportés. C'est d'abord, la procédure douanière de l'acquit-à-caution (prévu par l'article de l'arrêté du 2 octobre 1992), c'est-à-dire le paiement d'une caution forfaitaire qui n'est restituée au vendeur que lorsqu'il peut fournir la preuve de l'arrivée à destination et de la non-réexportation du matériel [46]. C'est ensuite la présence obligatoire d'une clause de non-réexportation (CNR) dans le contrat de vente (article 12 du décret de 1992) [47].

L'objectif principal de ces différentes procédures n'est pas la protection du secret. Il est d'abord politico-stratégique (évaluer si le renforcement des moyens militaires de l'État acheteur va dans le sens des intérêts français) et ensuite militaire (éviter de fournir des armes à des adversaires potentiels qui pourraient être amenés à les utiliser plus tard contre les forces françaises ou leurs alliés). Mais, de même qu'il s'agit de s'assurer du fait que la livraison de ces armes ne va pas à l'encontre de la sécurité de la France et de ses forces, ces procédures de contrôle permettent de s'assurer *a priori* du fait que cette livraison ne va pas entraîner la compromission d'un secret de défense.

La protection du secret fait donc partie – parmi d'autres – des critères pris en compte par la CIEEMG lors de son examen des demandes d'agrément [48]. Et cela est compréhensible, puisque, la plupart du temps, les industriels français exportent les mêmes équipements qu'ils ont conçus et vendus aux armées françaises. Une analyse détaillée de ces équipements par un client étranger malintentionné à l'égard de la France permettrait donc de connaître avec une certaine précision le niveau de performances et les faiblesses corrélatives des matériels équipant la défense française. Il est donc indispensable qu'un examen attentif des équipements à livrer et des données techniques qui les accompagneront fasse l'objet d'une évaluation au regard des nécessités de protection du secret.

Une lecture attentive des dispositions de l'arrêté du 2 octobre 1992 fixant la procédure d'exportation confirme, d'ailleurs, la préoccupation sous-jacente de la protection du secret. Son article 5 impose, notamment, un agrément avant toute prospection dès lors que celle-ci est *« accompagnée de la diffusion, sous quelque forme que ce soit, d'informations de nature à permettre ou à faciliter la fabrication ou la reproduction de ces matériels ou à en compromettre l'efficacité. »*

Et le même article soumet également à agrément préalable *« la cession à l'étranger de tous droits de propriété industrielle et de toute documentation relatifs aux matériels visés ci-dessus »* ainsi que *« l'échange, la cession ou la communication à l'étranger d'études ou de leurs résultats (y compris les prototypes) ainsi que des technologies de conception ou de fabrication directement associées à ces matériels ».*

Sachant que les caractéristiques des armements utilisés par les forces armées françaises font partie du domaine traditionnellement couvert par

---

[46] Sur cette procédure, cf. notamment, Mireille Couston, « Droit et pratique des marchés d'armement », *Droit et Défense*, n° 93/1, p. 23.

[47] Cf. notamment Jean-Luc Lagardère, « Les modalités de conclusion d'un contrat de vente d'armes » in *Le droit international et les armes*, colloque de la société française pour le droit international, Pedone, 1983, p. 197.

[48] Cf. Patrick Mercillon, « L'industrie d'armement » in Jacques Robert (sous la dir.) *L'esprit de défense*, Economica, Paris 1987.

le secret, on constate aisément que cette procédure des agréments préalables permet, en dehors du matériel lui-même, de s'assurer que l'exportation envisagée ne comportera pas de transferts d'informations secrètes ou permettant de faciliter la découverte d'un tel secret. Et cette préoccupation de préserver le secret se répercute, à son tour, sur le vendeur au travers d'une clause de secret inséré dans le contrat de vente et, dans le cas de certaines commandes importantes, au travers d'un *« accord intergouvernemental de sécurité »* parallèle à la signature du contrat.

Les protections « périphériques » des secrets technologiques ou économiques intéressant la défense

Pour compléter les mesures spécifiques prises au niveau des dépôts de demandes des titres de propriété industrielle ou de l'exécution des marchés classés de défense (cf. infra), plusieurs dispositifs annexes peuvent être, en effet, considérés comme contribuant périphériquement et indirectement à la protection de certains secrets technologiques ou économiques. Il s'agit essentiellement des mesures de protection du *« patrimoine national scientifique et technique »* en matière de contrôle des visites, des stages et des coopérations, du contrôle à l'exportation des produits et technologies sensibles et des limitations de communication de certaines informations à l'étranger.

Les tentatives de protection du patrimoine national scientifique et technique

Le Secrétariat général de la défense nationale et la DST – sensibilisées par les vulnérabilités économiques nouvelles de la France et par les menaces d'espionnage scientifique et technologique (notamment celles en provenance de l'URSS) ont conçu, aux lendemains de la crise pétrolière de 1973 [49], un concept différent de celui de secret de défense et à vocation principalement technologique : le *« patrimoine national scientifique et technique »*. La définition de cette notion lui conférait, en théorie, une très large portée, mais n'ayant jamais été précisée dans un texte réglementaire publié (mais uniquement dans des instructions confidentielles), ses contours n'ont pas été totalement fixés et nous devons nous en tenir aux interprétations qu'ont pu en donner des auteurs ayant exercé des responsabilités opérationnelles en la matière.

Pour le colonel Debrun, ancien cadre de la DPSD, le *« patrimoine scientifique et technique »* devait être vu comme un sous-ensemble d'un concept plus général de *« patrimoine national »* :

> *« Le patrimoine national correspond à l'ensemble des informations qui concernent les intérêts essentiels de l'État (économiques, diplomatiques, scientifiques, industriels ou commerciaux) dont le regroupement ou l'exploitation peut éventuellement conduire à la découverte d'un secret*

---

[49] Cf. Rémy Pautrat, « L'intelligence économique : un nouveau défi et un grand enjeu pour la France », *Défense - Revue de l'Union des associations d'auditeurs de l'IHEDN*, n° 65, septembre 1994, p. 46.

de défense nationale ou nuire à celle-ci, et qui justifient des mesures de protection sectorielles. » [50]

Cette présentation du patrimoine national faisait ressortir son large spectre (dépassant largement le seul domaine technologique et dont la définition comporte des affinités fortes avec celle adoptée ultérieurement par le nouveau Code pénal en ce qui concerne les intérêts fondamentaux de la nation). Mais on doit également constater la difficulté qu'il y avait, à l'époque, à distinguer cette notion de celle des « secrets par extension » (cf. articles 75 et 76 de l'ancien Code pénal). En revanche, la définition qu'il donnait du *« patrimoine scientifique et technique »* – proche de celle fournie par les textes réglementaires non publiés, en particulier l'instruction interministérielle n° 486 – se limitait aux seuls aspects technologiques, mais se distinguait plus clairement de la notion de secret de défense :

« D'une manière générale, par patrimoine scientifique et technique, il faut entendre tout savoir, quel que soit son support, tout savoir-faire, tout matériel intéressant non seulement le domaine strictement entendu des intérêts militaires de la défense (qu'il convient de protéger pour conserver notre indépendance ou notre avance) mais encore tout acquis dans les domaines scientifiques et techniques dont la connaissance par un pays étranger ferait perdre à la France un avantage dans un secteur concourant à sa puissance et à son indépendance et pourrait ainsi nuire indirectement à la défense nationale (considérée dans son acception globale). » [51]

Avec cette définition, on perçoit l'idée centrale de la protection du patrimoine : assurer au-delà de la protection directe des secrets de défense (dont la divulgation nuirait directement à la défense), une protection indirecte des intérêts nationaux en essayant de conserver une certaine confidentialité à certaines informations scientifiques et techniques (dont la divulgation nuirait à la position de la France, et donc – indirectement – à la défense nationale).

Mais un tel objectif a rencontré, dès sa formulation, des difficultés théoriques et juridiques. Comme l'expliquait Jean-Pierre Bansard, officier alors en poste au SGDN, dans un article paru en 1993 et consacré à la protection du patrimoine et à son évolution :

« La notion même de patrimoine national implique qu'il existe des droits de propriété sur un ensemble de biens détenus par la collectivité nationale. Ce sont alors ces droits de propriété qui légitiment les mesures de protection du bien collectif. Or (...) la connaissance scientifique est, par essence, rebelle à toute appropriation individuelle ou nationale. Il semble donc que la notion même de « patrimoine scientifique national » soit intrinsèquement paradoxale, ce qui constitue dès l'abord un indice assez peu favorable quant à la simplicité de la mission de protection confiée au SGDN. » [52]

---

[50] Henri Debrun, « Le secret de défense » in Jacques Robert (dir.), *op. cit.*

[51] H. Debrun, *op. cit.* Idem in Gérard Vial, « La sécurité du CEA - Une réponse aux diverses menaces de l'entreprise », *Réalités Industrielles/Annales des Mines*, octobre-novembre 1989, p. 132.

[52] Jean-Pierre Bansard « La protection du patrimoine scientifique et technologique national : de la théorie à la pratique d'hier à aujourd'hui » *in* Bertrand Warusfel (dir.), *Industrie, Technologie et Défense*, Travaux du Centre Droit et Défense, La documentation Française, 1993, p. 101.

La protection du patrimoine cumule, en effet, les handicaps juridiques. Elle présuppose en effet que la collectivité nationale veuille se prévaloir de certains droits sur des éléments intellectuels dont la propriété appartient pour l'essentiel à des personnes privées (entreprises, laboratoires, chercheurs, ...). Or, ces droits que réclame l'État ne peuvent pas être, comme on l'affirme parfois un peu hâtivement au SGDN [53], de véritables droits de propriété : il s'agirait plutôt, au mieux, d'une sorte de *« servitudes »* grevant les informations en question, mais dont le régime juridique serait assez complexe.

Il semble par ailleurs que l'administration n'ait jamais pu donner un contenu juridique et pratique réel à cette notion. Tout au plus, s'est-elle contentée de rattacher prudemment ce concept à des procédures déjà existantes (protection des marchés classés de défense, mise au secret des demandes de brevet) ainsi qu'à celle – déjà évoquée – du contrôle des visites et des stages. Et aujourd'hui le concept même de patrimoine national scientifique et technologique paraît plus ou moins abandonné. C'est ainsi, par exemple, qu'un responsable de la DST reconnaît dans un article récent que *« le concept même de patrimoine vole en éclat, et, partant, la protection de ces intérêts par l'État devient de plus en plus difficile, voire même utopique »* et semble lui préférer celui de *« sécurité économique active, concept dont la DST a été l'un des inventeurs »* [54].

Le contrôle des exportations de matériels et technologies à double usage

Outre les matériels de guerre proprement dits, la France, comme la plupart des pays occidentaux, exerce des contrôles à l'exportation sur d'autres types de produits ou de technologies pouvant avoir un usage militaire indirect.

Historiquement, la France a commencé par participer, dès la création du COCOM (COordinating COMmittee) en 1949, à la concertation des pays occidentaux regroupés sur l'initiative des États-Unis au sein de cet organisme. Ce comité dissous le 31 mars 1994 regroupait à la date de sa disparition dix-sept pays, soit l'ensemble de l'Alliance Atlantique – sauf l'Islande – plus le Japon et l'Australie. Il a eu comme unique fonction d'exercer un embargo sur les exportations d'une série de produits et de technologies militaires, nucléaires mais aussi – et surtout – civiles à double usage (civil et militaire) à destination de l'URSS, de la Chine et de leurs principaux satellites. À ce titre, la France a publié et tenu à jour pendant environ quarante années une liste commune établie par le COCOM de produits et technologies soumis à contrôle, sous la forme d'un *« avis aux importateurs et exportateurs relatif aux produits et technologies soumis au contrôle de la destination finale »* [55].

---

[53] Dans une synthèse du SGDN, le patrimoine scientifique et technique est présenté comme *« un bien exclusif de la communauté nationale »* (SGDN, *Bulletin de sécurité de défense*, n° 9, janvier 1995, p. 2).

[54] Eric Bellemin-Comte, « La protection du patrimoine économique, technologique et scientifique français : volet défensif de l'intelligence économique », *L'Armement*, décembre 1997-janvier 1998, p. 156.

[55] Sur ces procédures de contrôle de la destination finale, cf. Bernard Chantebout & Bertrand Warusfel (dir.) *Le contrôle des exportations de haute technologie vers les pays de l'Est*, Masson, 1988.

Par ailleurs, la France participe, depuis leur origine, aux différentes initiatives internationales destinées à limiter la prolifération de certaines technologies et armes de destruction massive. C'est ainsi que la France est membre du *Nuclear Supplier Group* (dit « *Club de Londres* ») [56] qui regroupe les principaux exportateurs de produits et technologies nucléaires civils, du *Missile Technology Control Regime* (MTCR) mis en place pour limiter la prolifération des armes balistiques [57] et de l'*Australia Group*, groupe informel consacré au contrôle des exportations de produits chimiques et biologiques à double usage [58].

L'ensemble des produits et technologies contrôlés au titre de ces différents régimes et de leurs listes respectives est désormais regroupé au sein d'une liste unique de contrôle des produits et technologies à double usage mise au point par les États membres de l'Union européenne dans le cadre d'une réglementation commune européenne fixée par le règlement du 19 décembre 1994 [59]. Cette réglementation commune a permis d'harmoniser les politiques des différents États membres et de faire disparaître les restrictions au commerce intra-communautaire qui résultaient précédemment de ces contrôles. Elle s'est donc intégralement substituée à la réglementation française antérieure – dite de « *contrôle de la destination finale* » (CDF).

Outre cette réglementation européenne qui assure un contrôle harmonisé sur les exportations extra-communautaires tout en permettant la libre circulation au sein de l'Union de la quasi-totalité des produits et technologies à double usage, le domaine des contrôles des exportations a connu – depuis la disparition du COCOM – une nouvelle étape de son évolution, avec la conclusion le 19 décembre 1995 de l'Arrangement de Wassenaar, qui est entré en vigueur en juillet 1996.

Cet accord qui regroupe actuellement trente-trois États (soit – outre les pays de l'ancien COCOM – certains autres pays industrialisés ou anciens membres du bloc de l'Est, comme la Hongrie, la Pologne, la Russie, la Slovaquie et la République tchèque) organise le contrôle d'un ensemble de biens ou technologies civiles à double usage ainsi que des matériels de guerre. Chaque pays membre s'y est engagé à ne pas autoriser de telles exportations vers les pays dont « *le comportement*

---

[56] Sur le NSG et la mise en place, en France, d'une instance de décision interministérielle spécialisée, le GIR (Groupe Interministériel Restreint), lui-même placé sous l'autorité d'un Conseil de Politique nucléaire extérieure, cf. Simone Courteix, *Exportation nucléaires et non-prolifération*, Economica, 1978.

[57] En France, la plupart des produits relevant de la liste MTCR (systèmes capables de projeter une charge utile de plus de 500 kg à plus de 300 km) étaient déjà pris en compte par la liste des matériels de guerre (cf. supra) et par la liste établie par l'ancien COCOM, le Gouvernement français n'avait donc pas jugé utile de publier une liste spécifique (à l'exception d'un court complément paru au *JORF* du 10 novembre 1990).

[58] Par ailleurs, les industriels français sont astreints à toutes les interdictions de fabrication et d'exportation découlant de la Convention de Paris sur l'interdiction des armes chimiques du 15 janvier 1993.

[59] Règlement (CE) n° 3381/94 du Conseil, du 19 décembre 1994, instituant un régime communautaire de contrôle des exportations de biens à double usage, *JOCE* L 367 du 31 décembre 1994, dont le contenu de la liste de contrôle a été modifié en 1996, en 1998, puis en 2000. Pour un commentaire de ce règlement, cf. Bertrand Warusfel, « Le règlement communautaire sur les produits et technologies à double usage et sa mise en œuvre en France », *Droit et Défense*, n° 95/3, pp. 53-57.

irresponsable menace la paix et la sécurité internationale ». Et bien que ne faisant pas l'objet d'une liste officielle, les pays visés par ce nouvel embargo multilatéral seraient principalement : la Corée du Nord, l'Iraq, l'Iran et la Libye.

S'ajoutant ainsi aux trois autres « clubs » de non-prolifération déjà évoqués, l'arrangement de Wassenaar confirme bien la nouvelle orientation prise depuis la chute de l'URSS par les contrôles des technologies à double usage : il s'agit de plus en plus de contrôles Nord-Sud, dont les finalités sont plus le maintien de la stabilité mondiale et la non-prolifération des armes de destruction massive que la simple sécurité nationale [61].

Jusqu'à présent, les systèmes de contrôle mis en place par les Occidentaux étaient l'œuvre d'un groupe restreint de nations développées qui exerçaient leur défiance à l'encontre de quelques pays *« visés »* limitativement identifiés au travers de restrictions d'exportation portant sur des listes de produits et technologies précisément définis. La transformation du contexte international a bouleversé ce schéma et un nouveau modèle de contrôle est en train d'émerger en marge des tentatives d'instauration d'un *« nouvel ordre international »*. Mais il est, d'ores et déjà, certain que cette nouvelle donne des contrôles ne permettra plus à chaque Gouvernement d'utiliser ces procédures pour protéger la périphérie de ses secrets technologiques de défense.

Les règles relatives à la communication d'informations à des personnes étrangères

Bien que les informations non secrètes soit, par principe, libres de franchir les frontières, le Gouvernement français a fait adopter par le Parlement en juillet 1980 une loi restreignant – sous peine de sanctions pénales – la transmission de certaines informations non secrètes à des personnes de nationalité étrangère [62].

Ce texte qui modifiait une loi de 1968 relative à la communication des informations concernant le commerce maritime, a visé deux cas distincts de transmission vers l'étranger de *« documents et renseignements d'ordre économique, commercial, industriel, financier ou technique »*.

Dans le premier cas, le nouvel article 1er modifié de la loi du 26 juillet 1968 édicte – *« sous réserve des traités ou accords internationaux »* [63] – une interdiction applicable à toute personne physique ou morale de

---

[60] Cf. dépêche AFP du 19 décembre 1995. Les « éléments initiaux » convenus entre les membres les 11 et 12 juillet 1996 sont consultables sur le site Internet www.wassenaar.org et reproduits en annexe du rapport parlementaire n° 2334 précité.

[61] Sur cette évolution de la philosophie des contrôles, cf. Bertrand Warusfel, « La prolifération des technologies sensibles vers le Sud : menaces et perspectives de contrôle », *Cultures et conflits*, n° 2, L'Harmattan, 1991.

[62] Loi n° 80-538 du 16 juillet 1980 relative à la communication de documents et renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères, *JORF*, 17 juillet 1980, p. 1799.

[63] L'exécution d'une commission rogatoire internationale, conformément aux dispositions fixées par les accords internationaux relatifs à la coopération judiciaire, rentre dans le cadre de cette exception au principe de l'interdiction de livraison d'informations à des fonctionnaires étrangers (cf. sur ce point l'opinion de Mme M. Hiance, *op. cit.*, p. 47).

nationalité française ou résidant en France [64]. Elle s'applique à la communication *« par écrit, oralement ou sous autre forme, en quelque lieu que ce soit »*, des informations susvisées dès lors que :

– cette communication est *« de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public* [65]*, précisés par l'autorité administrative en tant que de besoin* [66] *»*;

– et qu'elle est effectuée au profit d'*« autorités publiques étrangères »* [67].

Le second cas de communication prohibée par la loi du 16 juillet 1980 (nouvel article 1er *bis* de la loi du 26 juillet 1968 modifiée) présente des caractéristiques différentes à deux niveaux :

– concernant les auteurs de l'infraction, ne sont plus seulement visés les détenteurs d'information (comme précédemment) mais aussi les « chercheurs » d'information et ne sont plus concernées seulement les relations entre français et fonctionnaires étrangers, mais aussi les communications entre toutes personnes, quelles que soit leur nationalité ou leur résidence;

– concernant les informations communiquées, il s'agit toujours du même type d'informations mais il est n'est plus nécessaire de prouver que leur communication porte préjudice aux intérêts nationaux, le seul critère étant que lesdites informations tendent *« à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci »*.

Cette seconde infraction – punie des mêmes peines que la précédente (deux à six mois d'emprisonnement et 10.000 F à 120.000 F d'amende) – a été conçue principalement pour opposer un rempart légal à la pression des procédures judiciaires américaines [68]. Mais elle pourrait couvrir également des cas de procédures étrangères relatives à des faits couverts en France par le secret de défense.

L'ambiguïté du « potentiel scientifique et économique » protégé par le nouveau Code pénal

Parmi la liste des intérêts fondamentaux de la nation donnée par l'article 410-1, le législateur a choisi de mentionner *« son potentiel scientifi-*

---

[64] Cet article a fait l'objet d'un arrêté d'application spécifique concernant les entreprises de transport et de travail aérien (arrêté du 20 novembre 1980).

[65] On relèvera ici la similitude d'inspiration avec la définition désormais donnée par le nouveau Code pénal concernant les intérêts fondamentaux de la nation.

[66] Ainsi est affirmé un droit régalien de l'administration à définir elle-même les cas dans lesquels la communication serait contraire aux intérêts nationaux (ce qui revient à donner au pouvoir réglementaire la possibilité de définir le champ d'application de l'infraction). Cette méthode paraît généralement suspecte aux juristes : le professeur Gavalda la relevait déjà dans un texte antérieur (en l'occurrence le décret du 27 février 1963 relatif aux autorisations données aux entreprises au titre de la défense économique) et y voyait *« une sorte de secret à contenu variable »* (Christian Gavalda, « Le secret des affaires », in *Mélanges offerts à René Savatier*, Dalloz, 1965, p. 297).

[67] L'application n'est pas étendue – comme dans le nouveau Code pénal – aux organisations non-gouvernementales étrangères, ni aux organisations *« sous contrôle étranger »*.

[68] L'origine de cette disposition aurait été la crainte d'entreprises industrielles françaises d'avoir à se soumettre aux procédures américaines de « discovery » dans le cadre de procès de propriété industrielle (cf. Axel Casalonga, « Le secret et les professions de la propriété industrielle », in Centre Paul Roubier, *op. cit.*, p. 28). Elle n'aurait été cependant invoquée qu'une fois – et sans grand effet – devant la Cour de district de l'Illinois en 1984 (Graco v. Kremlin & SKM –

que et économique ». Par cette terminologie, le nouveau Code pénal a reconnu une certaine filiation avec le concept de « *patrimoine scientifique et technique* », déjà évoqué.

Mais il l'a, en apparence, élargi puisque le potentiel économique se trouve placé sur le même plan que le potentiel scientifique, ce qui évite de restreindre le champ de la protection aux seules données techniques et permet de l'étendre à des informations tant commerciales, industrielles que financières.

Pourtant, le paradoxe veut qu'en retenant ces deux termes, le législateur a sans doute procédé également à une involontaire limitation, dans la mesure ou il a choisi le seul terme de « *scientifique* » au détriment de tout autre qualificatif (telles que, par exemple, « *technique* » ou « *technologique* »). Il y a, en effet, de grandes différences entre la science et la technologie. Des différences de niveau, tout d'abord, entre un processus amont (la recherche scientifique) et une étape plus en aval (l'innovation technologique) dont la réalisation ne résulte pas de la seule maturation du savoir scientifique, mais d'une dialectique beaucoup plus complexe avec d'autres éléments économiques, sociaux ou culturels. Mais il existe également une différence juridique essentielle entre le domaine scientifique, régi par le principe de liberté de la recherche, d'internationalisation du savoir et de non-appropriation privative et celui de la technologie, dominé par les mécanismes de protection de la propriété intellectuelle.

À cela s'ajoute le fait que les éléments constitutifs de ce « *potentiel scientifique et économique* » ne sont pas décrits. Or, il est évident que toutes les connaissances scientifiques ou techniques ne peuvent bénéficier d'une protection pénale au titre de la protection des intérêts fondamentaux de la nation. Il serait donc nécessaire de distinguer parmi elles celles qui possèdent les caractéristiques adéquates pour relever de ce texte. On y trouve certainement la plupart des informations classifiées (mais qui sont très peu nombreuses en matière scientifique). En revanche, il n'apparaît pas facile de distinguer parmi les informations non classifiées celles qui sont protégées au nom des intérêts fondamentaux de la nation et celles qui ne le sont pas.

Et s'agissant des informations économiques, il faut aussi se demander si l'extension d'une telle protection pénale à des informations concurrentielles non directement associées à des activités gouvernementales ne pourrait pas être considérée (au regard des règles européennes et internationales) comme portant atteinte à la concurrence.

Il est donc permis de penser qu'en l'absence de toute intervention réglementaire en la matière fournissant plus ou moins directement des critères formels ou matériels d'évaluation du contenu de ce potentiel scientifique et économique, la jurisprudence pénale restera très timide en la matière et n'étendra pas largement l'application de ce concept au-delà du type d'informations dont la compromission était déjà réprimée par les anciens articles 77 ou 80.3° du Code pénal [69].

---

222 USPQ, 986-1984, cité par Pierre Veron, « Le secret et les procédures juridictionnelles en matière de propriété industrielle », in Centre Paul Roubier, *op. cit.*, p. 76).

[69] Madame Nicole Catala – députée et professeur des facultés de droit – n'hésita pas, lors du débat parlementaire sur le projet d'article 410-1 nCP, à affirmer que la formule relative aux

Le ferait-elle, d'ailleurs, que cela créerait, en matière de protection de la confidentialité des informations économiques et technologiques non classifiées, une situation de disparité juridique très aiguë entre :

– certaines informations non classifiées qui seraient ainsi protégées par des incriminations lourdement sanctionnées (entre sept ans d'emprisonnement et vingt ans de détention criminelle, suivant les infractions, c'est-à-dire plus lourdement que s'il s'agissait de la violation d'un simple secret de défense);

– l'ensemble des autres informations non classifiées qui ne bénéficient que de la protection très partielle qu'offre le droit français aux différentes formes des *« secrets d'affaires »* (ce qui se résume essentiellement à la protection des secrets de fabrique [70] et à certains aspects de la jurisprudence sur la concurrence déloyale [71]).

On relèvera d'ailleurs, à ce sujet, l'approche très différente retenue par le législateur fédéral américain avec l'adoption en 1996 de l'Economic Espionage Act. Cette loi protège pénalement tous les secrets d'affaires (trade secrets) – sans distinction de nature – et aggrave les sanctions encourues (15 ans au lieu de 10 ans d'emprisonnement) lorsque ces secrets sont compromis au profit *« d'un gouvernement, d'une organisation ou d'un agent étranger »* [72]. Mais ce faisant, le législateur américain a choisi d'extrapoler son dispositif contre l'espionnage économique d'État à partir de la protection des secrets d'affaires (soit une approche de bas en haut), au contraire de la démarche française qui par l'article 410-1 nCP a tenté de prolonger la protection des secrets de l'État vers le bas, sans pour autant oser instaurer un véritable secret d'entreprise en droit pénal français.

LA MUTATION DES ACTEURS DU SECRET : LA PROTECTION DU SECRET AU SEIN DES ENTREPRISES

Si le contenu du secret évolue, il en va de même pour ses producteurs et ses détenteurs. Alors que le système classique de protection a été conçu en fonction d'un secret né à l'intérieur de l'administration, géré par elle et seulement ponctuellement confié à des personnes extérieures, la nouvelle réalité économique et stratégique conduit à un renversement profond de la perspective.

Le nouveau contexte économique et stratégique est, en effet, caractérisé par la diversification et l'hétérogénéité des acteurs. Et l'un des aspects les plus importants et les plus frappants de cette évolution concerne la

---

« intérêts essentiels du potentiel scientifique et économique » débouchait sur *« une incrimination pénale floue* (qui) *laisse une trop grande marge d'appréciation au juge et une trop grande marge d'incertitude aux justiciables »* (*Assemblée nationale*, débats, 1re séance du 7 octobre 1991).

[70] Protection assurée par l'article L. 152-7 du Code du travail, auquel renvoie l'article L. 621-1 du Code de la propriété intellectuelle.

[71] Cf. notamment, Christian Gavalda, *op. cit.*, p. 292; Miroslav Kovarik, « Un aspect particulier du droit des affaires en France : l'espionnage économique et industriel », *Les Petites Affiches*, nº 84, 14 juillet 1986 (1re partie), p. 22; Corine Van Den Bussche, « La protection pénale contre l'espionnage des secrets d'affaire », *Les Petites Affiches*, nº 135, 10 novembre 1995 et nº 136, 13 novembre 1995.

[72] Economic Espionage Act of 1996, § 1831 (traduction française in *Droit et Défense*, nº 97/1, note Warusfel, pp. 64-66).

place majeure prise aujourd'hui par l'entreprise privée, acteur essentiel non seulement de l'économie marchande, mais aussi de la recherche scientifique et technologique, des relations sociales, des services collectifs, de la culture et des relations internationales. Concernant la protection du secret de défense, cela se traduit par l'importance pratique des procédures de protection du secret dans les marchés classés de défense.

Le recours au contrat pour transposer la protection du secret dans un contexte industriel et commercial

Le secret de défense étant, à l'origine, un secret de l'État (voire un « secret d'État »), sa protection a été conçue pour être assurée dans un cadre administratif de droit public. Ce cadre administratif présente, d'ailleurs, par nature, quelques avantages pour la préservation du secret : sélection, stabilité et permanence des personnels, règles spécifiques de loyalisme et de réserve applicables statutairement à ceux-ci, importance des structures hiérarchiques, absence d'intérêts privés divergents. Dès lors, l'accès au secret de personnes privées situées hors de l'administration et obéissant à des modes d'organisation et à des logiques de comportement différents, pose un problème de fond : comment reproduire dans un environnement différent (celui de l'entreprise en situation concurrentielle) un niveau de protection équivalent à celui supposé acquis au sein des services publics ?

Le dispositif des marchés classés de défense a été mis en place pour apporter une réponse pratique à cette interrogation. Son principe est simple : transposer au sein de l'entreprise les mécanismes de protection du secret utilisés dans les services étatiques, en utilisant le contrat (en l'occurrence le marché public conclu entre la personne publique et l'entreprise) comme substitut aux règles statutaires et réglementaires directement applicables au sein de l'administration.

Ce passage par la voie contractuelle pour assurer la protection du secret à l'intérieur des entreprises travaillant pour la défense, s'est imposé d'autant plus facilement qu'il s'agit le plus souvent de marchés d'armements. Ces marchés présentent, en effet, une double particularité juridique :

– il s'agit, généralement, de marchés industriels (au sens du Code des marchés publics et du Cahier des clauses administratives générales – Marchés industriels, CCAG/MI), dans lesquels l'Administration exerce une surveillance constante sur son contractant;

– la passation de ces marchés ayant trait à une activité de conception et de fabrication d'armement est soumise à autorisation préalable de l'administration, conformément aux dispositions du décret-loi du 18 avril 1939 (cf. supra) et à l'article 238 du Code des marchés publics qui précise que *« les titulaires de marchés de matériels de guerre passés par les administrations sont soumis aux contrôles définis par les textes relatifs au régime des matériels de guerre, armes et munitions »*.

On comprend bien que dans ce contexte des marchés d'armement, doublement contrôlés par l'État au titre de la réglementation des marchés et de celle des matériels de guerre, il est aisé d'introduire un troisième niveau de contrainte, celui du secret de défense. Les structures juridiques de l'autorisation préalable et de la surveillance *in situ* existant déjà, la

protection du secret s'est simplement glissée dans le dispositif préexistant, au risque de s'y confondre parfois [73].

Les caractéristiques d'un marché classé de défense

La notion de marché classé, comme la plupart de celles ayant trait à la protection du secret de défense, ne trouve pas son origine dans des textes législatifs ou réglementaires publiés. Absente du Code des marchés publics, elle n'apparaît directement que dans des instructions interministérielles et ministérielles non publiées et, indirectement, dans le contenu de certains CCAG.

La définition du marché classé (dit aussi parfois improprement « marché classifié ») est très simple : *« Un marché classé de défense nationale est un marché qui comporte des informations dites classifiées »* [74]. Le fait d'appartenir à cette catégorie particulière de marchés emporte un certain nombre de conséquences qui sont explicitées dans les instructions spécialisées (l'instruction interministérielle 2000, ou encore – au ministère de la défense – l'instruction ministérielle 2500). Mais elles sont aussi évoquées sous une formulation plus discrète dans les clauses des CCAG relatives à la sécurité.

Si nous prenons le CCAG/MI (utilisé notamment dans tous les programmes d'armement) [75], l'article 6.3 régit, en effet, le marché dès lors *« qu'il présente, en tout ou partie, un caractère secret, soit dans son objet, soit dans ses conditions d'exécution »*, ce qui correspond à la définition donnée plus haut du marché classé dont le critère est la présence d'un secret. Cet article impose à l'entreprise contractante deux niveaux d'obligation :

– d'une part, respecter les *« obligations générales relatives à la protection du secret, notamment à celles qui concernent le contrôle du personnel, ainsi qu'aux mesures particulières de protection à observer pour l'exécution du marché. »* (art. 6.33) [76] ;

– d'autre part et plus précisément *« prendre toutes dispositions pour assurer la conservation et la protection des éléments du marché qui revêtent un caractère secret »*, *« maintenir secret tout renseignement intéressant la défense dont il peut avoir eu connaissance de quelque manière que ce soit, à l'occasion du marché »* et *« aviser sans délai la personne publique de*

---

[73] Cette similitude va si loin que le décret créant la DPSD (cf. supra) mentionne sa mission de protection du secret dans les *« marchés classés de défense nationale passés par le Ministère de la Défense conformément aux dispositions de l'article 238 du Code des marchés publics »* (art. 4 du décret du 2 avril 1982), confondant ainsi la notion de marché classé (liée à la protection du secret) et celle de marché d'armement soumis à autorisation préalable au titre du régime des matériels de guerre.

[74] Georges Herrmann, *Guide pour la sécurité industrielle*, chez l'auteur, 1983, p. 9.

[75] *Cahier des Clauses Administratives Générales applicables aux marchés industriels*, décret n° 80-809 du 14 octobre 1980.

[76] L'agent central de sécurité du groupe Matra résumait ainsi le contenu de ces obligations : « (les) *mesures de protection (qui) consistent : à rechercher la vulnérabilité du personnel; à mettre en place le contrôle et le filtrage des accès aux informations; à ériger des zones dites réservées; à sensibiliser l'ensemble du personnel et à responsabiliser chacun à son niveau; à appliquer strictement les mesures réglementaires* ». (Georges Herrmann, « La surveillance des transferts de technologie et la politique de sécurité des entreprises », in B. Chantebout & B. Warusfel (dir.), *op. cit.*, pp. 91-92).

toute disparition, ainsi que de tout incident pouvant révéler un risque de violation du secret » (art. 6.34).

En contrepartie, la personne publique intervient à double titre :

– lors de l'établissement du marché pour « *notifier au titulaire par un document spécial les éléments à caractère secret du marché* » (art. 6.32), lequel document précise notamment les « *obligations générales* » et les « *mesures particulières* » de protection du secret que devra respecter le titulaire (art. 6.33);

– lors de l'exécution du marché, en usant du « *droit d'agréer les préposés du titulaire ainsi que ceux de ses sous-traitants; elle peut également exiger à tout moment le remplacement de toute personne participant à l'exécution des prestations* » (art. 6.35).

De ce dispositif ressortent directement ou indirectement deux éléments caractéristiques du marché classé :

– la présence dans le contrat de clauses contractuelles de sécurité (généralement prévues dans les CCAG [77]) et d'une annexe de sécurité énumérant les éléments du marché qui possèdent un caractère secret, leur niveau de sensibilité respectifs et les mesures de sécurité qui leur sont applicables [78];

– un contrôle des autorités de sécurité visant à s'assurer de la qualité de la protection assurée par l'entreprise contractante : au préalable par l'habilitation de l'entreprise (cf. infra), de ses éventuels sous-traitants et de certains de ses salariés; par une vérification de l'aptitude physique de l'entreprise à mettre en œuvre les obligations de sécurité; et en cours d'exécution du marché par la vérification de la bonne application de ces obligations.

Mais ce dispositif des marchés classés dépasse le cadre des seuls marchés publics. Il existe, en effet, des contrats non considérés comme des marchés publics qui peuvent donner lieu à transmission et exploitation de données classifiées. On peut penser, par exemple, aux commandes dîtes « hors marché » (c'est-à-dire passées pour un montant inférieur au seuil fixé par le Code des marchés publics). Les directives gouvernementales précisent également qu'un marché de sous-traitance entre deux entreprises privées passé pour l'exécution d'un marché classé peut constituer lui aussi un marché classé.

Les conventions de recherche passée par les services de recherche de la Délégation générale pour l'armement [79] sont encore un autre exemple de ces contrats qui ne présentent pas le caractère de marchés publics

---

[77] Le contenu de l'article du 6.3 du CCAG/MI citée plus haut, se retrouve identiquement dans l'article 7.3 du CCAG/PI. En revanche, le CCAG/FCS ne comporte que la disposition obligeant le titulaire à se soumettre aux « *dispositions particulières que la personne publique lui a fait communiquer* » dès lors que les prestations sont à exécuter dans un lieu sécurisé et notamment dans un « *point sensible* » ou une « *zone protégée* » (article 6.2 du CCAG/FCS).

[78] Sur l'annexe de sécurité, cf. l'article 7 de l'instruction interministérielle n° 2000 du 1er octobre 1986, reproduit en annexe 1 in DGA, *Guide sur la sécurité de défense dans les programmes d'armement (nationaux et à l'étranger)*, n° 140/DEF/DGA/CAB/BS du 24 novembre 1984, pp. 15-16; également, G. Herrmann, *Guide pour la sécurité industrielle*, p. 10; Robert Carayon, *50 mots-clefs de la sécurité*, Privat, 1985, p. 212.

[79] Sur ces conventions et leur régime juridique, cf. Louis Favoreu, « Un contrat administratif d'un type nouveau ? Les conventions de recherche de la DGRST et de la DRME », *AJDA*, 1965, pp. 443 et s. et pour une analyse plus récente : Guillaume Drago, « Les conventions de recherche

mais peuvent constituer néanmoins un marché classé. Les conditions générales applicables à ces conventions reprennent, en effet, l'ensemble des dispositions principales évoquées plus haut et constituant les caractéristiques d'un marché classé. Leur article 18, consacré au *« caractère secret de la recherche »* dispose, en effet, que la convention doit préciser le *« degré de secret éventuel des informations »* dans un *« document contractuel de sécurité »*, reprend quasiment mot à mot le contenu des articles 6.3 du CCAG/MI et 7.3 du CCAG/PI (cf. supra) et précise, de plus, que le titulaire et le responsable scientifique reconnaissent avoir pris connaissance des instructions interministérielles sur la protection du secret [80].

L'habilitation des entreprises titulaires de marchés classés

L'un des préalables indispensables à l'exécution d'un marché classé est donc l'habilitation de l'entreprise (même si cela ne la dispensera pas de faire également habiliter toutes les personnes qui en son sein seront amenées à traiter les informations classifiées).

À partir d'une demande établie par l'autorité administrative contractante, d'un formulaire de renseignements décrivant la société et des dossiers d'habilitation individuelle de ses dirigeants et responsables de sécurité, une enquête est effectuée par un service spécialisé (de la même manière que pour les habilitations de personne physique : la DPSD est compétente pour les marchés classés du ministère de la défense et la DST pour les marchés des autres administrations). Cette enquête consiste essentiellement en la vérification des informations fournies dans le dossier et constitue – d'une certaine manière – une *« enquête de moralité »* appliquée à l'entreprise (il peut s'agir d'éviter, par exemple, que soit confié un marché classé à une entreprise dont la santé économique serait trop compromise, ce qui pourrait conduire les dirigeants à devenir *« vulnérables »* à des pressions extérieures [81]).

Mais au-delà des garanties que présentent l'état de l'entreprise et ses dirigeants du point de vue de la sécurité, l'autorité contractante ne peut accorder une décision favorable d'habilitation que si sont également réunies toutes les conditions prévues par le décret du 12 mars 1973 relatif à l'application du décret-loi du 18 avril 1939 concernant la fabrication et le commerce des armes et matériels de guerre, à savoir :

– pour une entreprise individuelle : appartenir à un français ;

– pour les sociétés de personnes : que tous les associés et gérants soient français ;

– pour les Sarl et les sociétés par actions et/ou en commandite : avoir tous les gérants, commandités, membres du conseil d'administration,

---

passées par le ministère de la Défense », in B. Warusfel (dir.), *Industrie, technologie et défense*, *op. cit.*, p. 65 et s.

[80] Article 18.2.1. des *Conditions générales applicables aux conventions de recherches non soumises aux dispositions du Code des marchés publics passées par la Direction des recherches, études et techniques (édition avril 1988)*, reproduites en annexe in G. Drago, *op. cit.*, p. 95.

[81] Dans une affaire d'espionnage technologique et d'exportation de produits sensibles (l'affaire Tavera), le président de la Cour d'Assises s'exclama : *« Si les PDG de sociétés en difficulté se mettaient à travailler pour l'URSS pour s'en sortir et laissaient racheter leurs firmes par les services secrets soviétiques, où allait-on ? »* (André Giresse & Philippe Bernert, *Seule la vérité blesse – L'honneur de déplaire*, Plon, 1987, réédition : Presses Pocket, 1988, p. 329).

du directoire ou du conseil de surveillance, de nationalité française, et avoir la majorité du capital détenue par des personnes de nationalité française.

Une décision favorable d'habilitation autorise les services gouvernementaux à passer avec l'entreprise des marchés classés, sous réserve que des visites sur le site d'exécution du marché permettent aux services de sécurité d'évaluer positivement l'aptitude physique de l'entreprise à mettre en œuvre efficacement les règles de sécurité et de protection du secret.

Par rapport au droit communautaire, cette procédure d'habilitation des entreprises contractantes de marchés classés ne paraît pas poser de problèmes particuliers lorsqu'elle s'applique à des entreprises travaillant sur des contrats d'armement (ce qui est le cas le plus souvent). En effet, dans ce cas, l'ancien article 223b du Traité de Rome (aujourd'hui, article 296b du Traité d'Amsterdam) s'applique automatiquement. Plus largement, la directive du 22 mars 1988 sur les marchés publics précise qu'elle ne s'applique pas *« aux fournitures, lorsqu'elles sont déclarées secrètes »*. Néanmoins, il faut garder à l'esprit que dans le cas d'un marché classé concernant un domaine non militaire (défense civile ou produit à double usage), le juge communautaire pourra être tenté d'apprécier le caractère nécessaire et proportionné du secret qui serait invoqué pour justifier une dérogation aux règles de concurrence et une discrimination en faveur des entreprises de nationalité française. La faiblesse juridique du recours au seul critère de nationalité et la perte de pertinence de celui-ci appliqué à des personnes morales est, d'ailleurs, un sujet de préoccupation pour les responsables de l'administration [82].

LA MUTATION DES SUPPORTS DU SECRET : SÉCURITÉ ET PROTECTION DU SECRET EN MILIEU INFORMATISÉ

Notre époque est marquée profondément, tant dans son économie que dans ses modes de travail et de vie, par le développement extrêmement rapide des moyens électroniques de traitement de l'information. Du point de vue des questions de sécurité et de défense, l'usage généralisé des systèmes d'information crée de nouvelles vulnérabilités qui obligent à modifier et à compléter les règles traditionnelles de protection du secret par des règles spécifiques applicables aux systèmes d'information.

Les nouvelles vulnérabilités induites par l'emploi des systèmes d'information

Par rapport aux règles classiques régissant la protection des supports du secret, l'utilisation des systèmes de traitement de l'information induit quelques transformations qualitatives essentielles :

---

[82] *« Les difficultés qui concernent la nationalité des personnes physiques ne sont rien au regard de celles qui sont soulevées par les personnes morales privées telles que les sociétés et groupes industriels. En effet, les groupes industriels sont la plupart du temps des entités supranationales disposant de filiales dans un grand nombre de pays. Comment doit-on considérer ces filiales ?* (...) *en fait, la notion même de nationalité d'une société semble vouée à perdre son sens, tout du moins son sens actuel. »* (J.-P. Bansard, *op. cit.*, pp. 116 et 117). La question de l'harmonisation des règles d'habilitation des sociétés européennes de défense est donc l'un des thèmes de travail retenus par les six pays européens qui ont signé le 6 juillet 1998 une « lettre d'intention » sur les restructurations en matière de défense.

– la dématérialisation des informations banalise les différentes informations (qui sont toutes sous forme électronique), rend leur identification physique plus difficile (il n'y a plus de marque physique aisément repérable de leur présence)[83] et en accroît considérablement la facilité de duplication;

– la délocalisation des informations via les réseaux de communication comme l'Internet, est le second aspect de la mutation technologique des systèmes d'information. Alors que traditionnellement le transport et le traitement étaient deux actions autonomes et exclusives l'une de l'autre, dans un système d'information interconnecté la transmission de l'information est transparente et ne se distingue pas réellement des autres opérations de traitement. On accède donc à une information de la même manière qu'elle soit stockée physiquement sur place ou qu'elle soit située à l'autre bout de la planète. L'on perçoit alors toutes les fragilités qu'une telle situation induit dans les procédures traditionnelles de sécurité, qui reposent pour une partie importante sur le cantonnement et la surveillance physique des supports d'informations confidentielles;

– enfin, le développement des systèmes d'information se traduit par une dépendance croissante de toutes les fonctions sociales et productives par rapport au bon fonctionnement de ces systèmes. Cela rend donc vulnérables de nombreux secteurs de la vie collective aux risques d'indisponibilité des moyens de traitement de l'information et crée, de ce fait, des opportunités nouvelles de nuisance et, donc, des besoins de sécurité corrélatifs.

La typologie des atteintes à la sécurité des systèmes d'information

Les objectifs de la sécurité des systèmes d'information sont généralement classés en trois catégories concentriques[84] :

– le premier niveau de sécurité est celui de l'accessibilité (ou la disponibilité) qui se caractérise par le fait que le système doit être en permanence utilisable pour remplir les fonctions qui lui sont assignées;

– le second niveau de sécurité est celui de l'intégrité qui se caractérise par le fait que les données traitées et les programmes exécutés par le système ne peuvent pas subir d'altérations et qu'en conséquence l'utilisateur peut se fier en toute confiance aux résultats fournis par le système;

– le troisième niveau de sécurité est celui de la confidentialité qui se caractérise en ce que les données traitées par le système ne peuvent être portées qu'à la connaissance de personnes habilitées pour ce faire, à l'exception de toute personne extérieure. Ce niveau n'est, cependant, pas une exigence majeure pour toutes les activités. Dans beaucoup de domai-

---

[83] Suite à l'arrestation en 1979 d'un fonctionnaire du ministère britannique de la défense, John Barry Wagstaff, accusé d'avoir dérobé des cassettes contenant des données classifiées, l'enquête releva que la simple assimilation administrative de ces supports magnétiques à des documents écrits classifiés n'était pas suffisante, étant donné les différences d'usage, notamment en ce qui concerne le marquage. La commission de sécurité avait alors prescrit la mise en place de règles spécifiques de sécurité applicables aux moyens informatiques (cf. Report of the Security Commission, mai 1981, *HMSO*, Cmnd. 8235, Londres, pp. 8 et 9).

[84] Cf. par exemple, *Protection des informations sensibles ne relevant pas du secret de défense - Recommandations pour les postes de travail informatiques*, n° 600/SGDN/DISSI/SCSSI, janvier 1990, p. 3.

nes, l'information traitée n'est pas d'une nature suffisamment sensible par elle-même pour devoir être conservée complètement confidentielle et la demande d'accessibilité et d'intégrité est prioritaire. En revanche, dans certains cas (dont, bien entendu, ceux ayant trait à la protection du secret de défense), la confidentialité devient indispensable et prend alors le pas sur les deux autres niveaux.

Il est donc intéressant de classer les types d'atteinte à la sécurité des systèmes d'information en fonction des trois niveaux de sécurité décrits ci-dessus :

– les atteintes à l'accessibilité (qui regroupent tous les actes susceptibles de mettre le système hors d'état d'accomplir sa fonction) peuvent être de deux ordres : des atteintes involontaires (les risques accidentels) et des atteintes volontaires (le sabotage physique ou logique);

– les atteintes à l'intégrité se distinguent des atteintes à l'accessibilité par le fait que, pour atteindre leurs buts (à savoir affecter l'intégrité du traitement effectué par le système), il est nécessaire que le système demeure en état de fonctionnement apparent et que les altérations qu'il a subies ne soient pas aisément détectables. Pour l'essentiel, il s'agira également de sabotage logique affectant les processus de traitement du système, avec une variante, que nous appelons manipulation frauduleuse qui se distingue de la simple atteinte logique à l'intégrité du système par le fait que l'objectif recherché est que le système se mette à produire certains effets utiles aux intérêts de l'auteur de la manipulation;

– les atteintes à la confidentialité, consistant au sens large à obtenir de manière clandestine l'accès à des données dont l'utilisateur souhaite empêcher la diffusion et la reproduction, recouvrent essentiellement les différents agissements que l'on peut regrouper sous le terme d'espionnage électronique [85].

On peut ajouter à cette typologie des atteintes, quelques éléments – plus subjectifs – sur la typologie des auteurs de tels agissements. Ainsi, le Service central de sécurité des systèmes d'information (SCSSI, cf. infra) distingue les menaces en fonction du type de motivation : ludique, avide, terroriste ou stratégique [86]. Cette distinction entre les différentes catégories d'attaquants ne doit pas être comprise de manière rigide, dans la mesure où l'observation des atteintes constatées sur les systèmes d'information depuis plusieurs années permet de s'apercevoir qu'il peut y avoir des glissements d'un type de menace vers l'autre [87], et que, notamment « (la menace stratégique) *est d'autant plus sérieuse qu'il y a interpénétration entre les différentes menaces, l'expérience ayant montré qu'un certain*

---

[85] De nombreuses techniques peuvent être employées à cette fin. Cela va du simple accès physique au système en l'absence ou à l'insu de son utilisateur au branchement sur un câble ou une ligne de communication afin de l'écouter, en passant par la captation à distance des ondes électromagnétiques émises indirectement par la plupart des systèmes électroniques (cf. infra, nos développements sur la lutte contre les rayonnements compromettants).

[86] Cf. notamment Eric Meillan, *La sécurité des systèmes d'information - Les aspects juridiques*, Hermès, 1993, pp. 12-13.

[87] Cf. E. Meillan, *op. cit.*, p. 13.

nombre de pirates ludiques étaient en réalité manipulés par des services de renseignement » [88].

Les risques spécifiques menaçant la sécurité nationale

Les systèmes d'information ont toujours été un enjeu stratégique pour les États et les services publics qui en sont généralement des utilisateurs intensifs.

Citons, par exemple, dans le domaine militaire, les systèmes de commandement dénommés C^3I [89] ou, dans le domaine civil, les réseaux publics de télécommunications ainsi que les systèmes informatisés de supervision et de gestion des grands réseaux de transport et de distribution d'énergie. De même, les administrations publiques sont à la fois un des lieux privilégiés de la recherche scientifique et technique (activités fortement utilisatrices de systèmes d'information, notamment de supercalculateurs et de réseaux à haut débit [90]) et le principal lieu de collecte et de stockage automatisé des informations nominatives, économiques et sociales (notamment au travers des fichiers des services du Ministère des Finances et de l'INSEE).

Dans ces conditions, la sécurité de ces systèmes d'information et de communication est essentielle pour la propre sécurité des activités publiques elles-mêmes. Et ce, y compris en matière de protection du secret, puisque, d'après une estimation administrative, environ 50 % des secrets de défense étaient déjà en 1987 traités ou échangés sous forme informatique [91]. Si on analyse donc, du point de vue des intérêts de l'État et de la sécurité nationale, les risques d'atteinte à la sécurité des systèmes décrits plus haut, on peut identifier trois types de risque qui paraissent spécifiquement importants de ce point de vue : celui de l'espionnage électronique d'informations classifiées, celui du sabotage des systèmes d'information vitaux et celui de la manipulation frauduleuse de données en vue d'induire en erreur les systèmes publics et leurs utilisateurs.

Le risque d'espionnage électronique en vue de recueillir des informations classifiées est l'un des plus anciens risques identifiés en matière d'usage de systèmes d'information par les autorités politiques et militaires. L'exemple historique majeur en est certainement celui de l'écoute et du déchiffrement de la quasi-totalité des communications militaires allemandes et japonaises durant la seconde guerre mondiale par les Alliés [92]. Il a

---

[88] Cf. Jacques Vincent-Carrefour (alors Délégué interministériel à la sécurité des systèmes d'information) in *Les cahiers de la sécurité intérieure*, IHESI/La Documentation française, n° 10, août-octobre 1992, p. 112.

[89] C^3I, acronyme anglo-saxon (*Command, Control, Communication and Intelligence*) désignant les systèmes intégrés de communication et de commandement.

[90] Citons notamment, en France, le réseau RENATER développé par France Telecom en partenariat avec la communauté scientifique et le Ministère de la Recherche et qui est, actuellement, l'un des supports importants de l'Internet en France.

[91] Cf. *Bulletin de sécurité de défense*, SGDN, n° 3, décembre 1987, p. 1.

[92] Sur la pénétration du système allemand Enigma, cf. notamment F. W. Winterbotham, *The Ultra Secret*, Weidenfeld & Nicholson, Londres, 1974, traduction française : *Ultra*, Robert Laffont, 1976; Antony Cave Brown, *Bodyguard of Lies*, Harper & Row, New York, 1975, traduction française : *La guerre secrète – le rempart des mensonges*, Pygmalion/Gérard Watelet, 1981 (particulièrement le Tome 1er : *L'origine des moyens spéciaux*); et pour la part importante qu'y ont jouée les services français : Gustave Bertrand, *Enigma*, Plon, 1973 et Paul Paillole, *Notre*

justifié – outre la conservation d'un secret très sévère sur ce dossier, durant de très longues années – la création d'organismes spécialisés dans la protection et l'attaque des systèmes d'information et de communication : le plus grand et le plus secret d'entre eux a été – et demeure – la National Security Agency (NSA) américaine, créée en novembre 1952, dont l'existence resta quasiment inconnue jusqu'à la fin des années soixante-dix [93] et qui dispose, aujourd'hui, de moyens techniques et financiers considérables.

La période de guerre froide a vu se développer l'utilisation intense des « sources techniques » (euphémisme généralement employé pour désigner les différentes formes d'espionnage électronique). Ainsi, la CIA installa, par exemple, un tunnel passant sous la ligne de démarcation avec le secteur soviétique de Berlin afin d'effectuer des écoutes sur les câbles téléphoniques reliant les forces soviétiques de la ville à leurs états-majors [94]. Mais cette opération fut rapidement dénoncée au KGB par le traître britannique Georges Blake [95].

Ce type de tentative de branchement clandestin paraît s'être perpétuée [96]. L'ambassade allemande à Moscou fut ainsi victime en 1964 d'un micro permettant d'intercepter avant chiffrement les télex destinés au ministère allemand des affaires étrangères [97]. Vingt ans plus tard, ont découvrit que les télex de l'ambassade de France à Moscou avaient été également piégés (sans doute, grâce à la complicité d'un chiffreur du Quai d'Orsay, recruté dès 1945 par le KGB [98]). La découverte en janvier 1983 de ce piratage du KGB serait d'ailleurs la cause directe de l'expulsion de France le 5 avril 1983 des quarante-sept diplomates soviétiques, (dont la liste fut établie grâce aux informations fournies à la DST par « Farewell » – cf. supra) [99].

Mais surtout dans le courant des années quatre-vingt plusieurs affaires, plus ou moins complètement élucidées, ont montré que des intrusions informatiques logiques (c'est-à-dire sans branchement physique et par le simple biais des réseaux de communication auxquels sont raccordés

---

agent chez Hitler, Robert Laffont, 1985. En ce qui concerne la pénétration des codes japonais : Ronald W. Clark, *The Man Who Broke Purple*, Weidenfeld & Nicolson, Londres, 1977; James Rusbridger & Eric Nave, *Betrayal of Pearl Harbor - How Churchill Lured Roosevelt into WWII*, Simon & Schuster, New York, 1991 (traduction française : *Trahison à Pearl Harbour - Comment Churchill a entraîné Roosevelt dans la Seconde Guerre Mondiale*, Pygmalion/Gerard Watelet, 1992).

[93] Cf. le premier ouvrage – très documenté – entièrement consacré à la NSA : James Bamford, *The Puzzle Palace - Inside the National Security Agency, A Report on America's Most Secret Agency*, Houghton Mifflin Company, 1982.

[94] Cf. David Martin, *The Wilderness of mirrors*, Harper & Row, New York, 1980, traduction française : *KGB contre CIA*, Presses de la Renaissance, 1981, pp. 102 à 124.

[95] Sur la trahison du tunnel par Blake, cf. notamment E. H. Cookridge, *Shadows of a Spy - The Complete Dossier on George Blake*, Leslie Frewin Publishers, Londres, 1967, p. 157 et 158; D. C. Martin, *op. cit.*, pp. 137 à 139.

[96] En 1985, la presse révéla par exemple qu'aurait été détectée et empêchée une tentative de branchement sur les câbles informatiques du ministère de la défense (*Le Figaro*, 11 juin 1985).

[97] Cf. John Barron, *KGB*, Elsevier Sequoïa, Paris/Berne, 1975, p. 24.

[98] La révélation de l'existence de cette « taupe » au service du chiffre diplomatique français provient des documents du transfuge Mitrokhin, cf. Christopher Andrew & Vasili Mitrokhin, *The Mitrokhin Archive - The KGB in Europe and the West*, Allen Lane & Penguin Press, London, 1999, pp. 608-609.

[99] Cf. notamment Jacques Attali, *Verbatim I 1981/1986*, Fayard, 1993, p. 382; *Le Point*, 8 avril 1985.

informatiques militaires ou directement liés à des activités de défense nationale. Parmi les sites informatiques français traitant éventuellement des informations classifiées, ayant fait – d'après la presse – l'objet de pénétrations, on peut citer :

– le centre de calcul vectoriel pour la recherche (C2VR) de l'École Polytechnique à Palaiseau en mars 1986 [100];

– le centre de calcul de l'EDF à Clamart en 1984 [101];

– différents systèmes informatiques appartenant au CEA [102];

– le système d'un autre organisme public français (non identifié) en décembre 1986 [103];

– en 1989, deux informaticiens français ont été arrêtés pour avoir pénétré illicitement dans plusieurs centaines de systèmes informatiques, dont celui de la Direction des Constructions Navales à Cherbourg [104].

À ces affaires purement françaises, s'ajoutent des affaires plus internationales (ce qui est normal, du fait de l'internationalisation des communications) et d'une plus grande portée. On se contentera de rappeler les trois principales :

– en septembre 1987, la presse a révélé que des « pirates » informatiques, en lien avec le groupe de Hambourg appelé le Chaos Computer Club (CCC), avaient pénétré le réseau SPAN reliant la NASA aux autres agences spatiales occidentales [105]. Ils auraient pénétré, par ce biais, 135 sites informatiques dans le monde entier et dans plusieurs cas il aurait été constaté la disparition ou l'altération de données confidentielles [106]. La police française détecta des intrusions du CCC dans les systèmes informatiques du CEA, de Thomson, de Philips-France et interpelle lors de sa venue sur le territoire français en 1988 le responsable du CCC Stephen Wernery [107];

– une enquête entreprise mi-1986 aux États-Unis à la suite d'un incident au Lawrence Berkeley Laboratory permit d'identifier un groupe de pirates ouest-allemands, qui furent accusés d'avoir pénétré de nombreux

---

[100] La Délégation générale pour l'armement confirma la pénétration tout en affirmant qu'aucune information classifiée n'était traitée sur cette machine qui ne servait qu'à la réalisation de calculs scientifiques ou techniques très partiels, et donc non confidentiels en eux-mêmes (cf. *Le Matin de Paris*, 18 juillet 1986 et 19/20 juillet 1986; *Le Monde*, 19 juillet 1986).

[101] Un stagiaire étranger employé durant l'été 1984 à la direction des études et recherches de l'EDF aurait permis aux soviétiques de se connecter à l'ordinateur central de l'établissement et d'y prendre connaissance de différentes informations techniques (*Le Parisien Libéré*, 6 juin 1986, pp. 2 et 3; *Le Monde*, 7 juin 1986).

[102] En 1984, Le Canard Enchaîné révéla avoir accédé par Minitel (sans doute grâce à une complicité intérieure) à une banque de données gérée par la CISI (filiale informatique du CEA) et contenant différentes informations plus ou moins confidentielles sur les activités du CEA, dont certaines sur des opérations sur le site de Muruoa, le planning de construction du cœur d'une centrale nucléaire ou sur des projets de laser « *classé secret* » (*Le Canard Enchaîné*, 28 novembre 1984, p. 3; *Le Monde Informatique*, 3 décembre 1984). Par ailleurs, un mini-ordinateur du département de recherche en physique des particules du CEA aurait été pénétré en 1986 (cf. *Le Matin de Paris*, 19/20 juillet 1986, p. 3).

[103] *Bulletin de sécurité de défense*, n° 3, *op. cit.*, p. 4.

[104] Cf. notamment *AFP*, 26 avril 1989.

[105] Le CCC a toujours nié avoir réalisé lui-même les piratages en question et prétendu avoir simplement été contacté par les « pirates » et avoir prévenu les services de sécurité (cf. *AFP*, 1er mars 1989).

[106] Cf. notamment, *Bulletin de sécurité de défense*, n° 3, *op. cit.*, p. 4.

[107] Cf. notamment *L'Express*, 11 mars 1988; *AFP*, 1er mars 1989.

centres informatiques militaires et aérospatiaux américains : la banque de données « Optimus » du Département de la défense, le Jet Propulsion Laboratory de Pasadena, le centre atomique de Los Alamos, ainsi que différents sites européens, notamment à l'Agence spatiale européenne, chez Thomson CSF, Philips France, au CERN ou au CNRS. Les enquêtes parallèles américaines, françaises et allemandes débouchèrent en mars 1989 sur l'inculpation de huit jeunes pirates allemands (dont trois furent arrêtés) et sur la démonstration – pour la première fois – de l'implication directe du KGB dans leur manipulation et leur exploitation [108];

– en 1988, la presse a révélé qu'un jeune informaticien avait été arrêté – puis relâché – par la police britannique pour avoir essayé d'effectuer du chantage auprès des sociétés IBM et Digital Equipment. Cette arrestation aurait permis de découvrir les indices de nombreuses pénétrations dans des bases de données appartenant à la défense britannique, à la NASA américaine et à plusieurs centaines d'entreprises ou laboratoires en Europe (dont Alcatel, SGS-Thomson, le CERN) [109];

– en 1995, un jeune français Anthony Zboralski était poursuivi par la justice et placé en détention provisoire pour avoir réussi à pénétrer sur le réseau de communication privé du FBI en usurpant l'identité du représentant de l'agence américaine à Paris [110].

À côté des risques d'espionnage électronique et informatique, les autorités de défense des pays occidentaux s'inquiètent des risques de sabotage des systèmes d'information vitaux. De tels risques peuvent prendre plusieurs aspects :

– le sabotage accidentel d'un système sensible à l'occasion d'une pénétration mal conduite (par exemple, effacement de certains fichiers);

– le sabotage volontaire à des fins mercantiles (par exemple de chantage), ou simplement ludiques;

– le sabotage volontaire d'un système à des fins terroristes [111];

– le sabotage volontaire comme moyen d'affaiblissement du pays en cas de crise ou comme préparatif ultime d'une éventuelle action armée.

Concernant le dernier point, la plupart des pays industrialisés ont notamment pris des mesures afin de « durcir » leurs principaux réseaux informatiques de communication et de commandement et les soustraire ainsi aux effets de l'impulsion électromagnétique (IEM) qui résulterait de l'explosion en altitude d'un explosif nucléaire (laquelle aurait pour effet la mise hors d'usage de tous les dispositifs électroniques dans un vaste

---

[108] Cf. notamment *AFP*, 3 mars 1989; *Paris-Match*, 16 mars 1989; *L'Express*, 10 mars 1989; *Le Monde*, 4 et 7 mars 1989. Quelques mois après, l'un de ces pirates, qui avait été « retourné » par les services allemands, a été retrouvé mort dans des conditions suspectes (cf. *Expertises des systèmes d'information*, n° 118, juillet 1989).

[109] Cf. *Le Quotidien de Paris*, 25 octobre 1988, citant le *Sunday Telegraph*. La similitude de certaines des sites visés peut faire croire à un lien avec l'affaire rendue publique l'année suivante en Allemagne (cf. infra).

[110] Cf. Jean Guisnel, *Guerres dans le cyberspace - Services secrets et Internet*, La Découverte, 1995, pp. 80-83; Le Monde, 10 juin 1995 (cf. également l'interview d'A. Zboralski, *Le Figaro*, 18 décembre 1997).

[111] La France a connu quelques rares cas de tentatives de terrorisme informatique d'origine anarchiste (notamment, un éphémère groupe dénommé CLODO qui commit plusieurs attentats matériels contre des sites informatiques).

rayon) [112]. Mais, dès le temps de paix, différentes manipulations sur les systèmes informatiques centraux de différents réseaux vitaux (communication, transport, énergie, ...) pourraient avoir les mêmes effets, et ce d'autant que les techniques informatiques actuelles permettent d'envisager la mise en place de « bombes à retardement » que l'on peut placer très discrètement dans les systèmes et qui pourraient être actionnées à distance le jour venu [113].

Le seul cas connu d'un sabotage effectif d'un système d'information gouvernemental a été rendu public en fin 1988 : un jeune étudiant américain, Robert T. Morris a introduit, par jeu, un virus informatique dans le réseau ARPANET (réseau de messagerie électronique géré par la DARPA, l'agence fédérale pour les projets technologiques de défense, et qui a servi de point de départ au réseau international Internet) qui s'est – par erreur – mis à proliférer jusqu'à bloquer le fonctionnement de 6.000 systèmes informatiques, dont plusieurs appartenant au Pentagone et à des agences fédérales américaines. Il a été poursuivi devant la justice américaine sur le fondement de la loi fédérale sur le piratage informatique [114]. À l'inverse, un magazine américain a pu affirmer, il y a quelques années, que les services de renseignement américains pratiquaient activement, non seulement la pénétration de systèmes d'information soviétiques, mais aussi leur sabotage à l'aide de virus informatiques [115].

Mais, plus encore que la violation de données confidentielles ou le sabotage de systèmes informatiques, l'une des principales menaces auxquelles sont exposés les systèmes d'information sensibles est la manipulation frauduleuse d'informations en vue d'induire en erreur soit les autorités, soit la population. De même que l'intoxication et la désinformation font partie intégrante du renseignement, la désinformation informatique devient un mode d'action offensif qui pourrait s'avérer très efficace.

Si l'on ne connaît pas d'exemple public de manipulation informatique à des fins d'intoxication en matière militaire ou politico-stratégique, il est facile d'imaginer de telles hypothèses [116]. Par exemple, il y a une dizaine d'années, une fausse information diffusée sur un service de messagerie Minitel boursière avait entraîné une chute de plus de 30 % de la valeur des actions d'une entreprise dont on avait annoncé faussement la rupture d'avec son principal fournisseur.

Dans le contexte de la vie économique et de la mondialisation actuelle, il n'est pas difficile d'imaginer que la transmission de fausses

---

[112] Cf. notamment, Bertrand Warusfel, « Sécurité informatique et secret de défense », *Défense nationale*, février 1986, p. 87.

[113] Cette crainte – bien réelle – des « bombes logiques » a donné lieu, dans le public à plusieurs alertes au virus informatique et à un roman d'anticipation (Thierry Breton & Denis Beneich, *Softwar - La guerre douce*, Robert Laffont, 1984).

[114] Cf. notamment *AFP*, 3 août 1989; *Paris-Match*, novembre 1988, p. 106. Pour l'anecdote, Robert T. Morris serait le fils d'un des responsables de la NSA en charge du National Computer Security Center (*Le Quotidien de Paris*, 7 novembre 1988).

[115] Le magazine *Time* cité par l'*AFP*, 13 mars 1989.

[116] Rappelons, pour l'anecdote, qu'Alexandre Dumas a imaginé ce qui est sans doute le premier cas de désinformation par le biais d'un système de communication : dans le chapitre LXI du *Comte de Monte-Cristo*, son héros se venge de son ennemi Danglars, spéculateur enragé, en soudoyant le servant d'une station du télégraphe de Chappe afin qu'il transmette à Paris une fausse nouvelle concernant l'évolution de la situation en Espagne, conduisant ainsi son ennemi à

informations via les réseaux de communication peut avoir des effets rapides et mettre en échec la vigilance des spécialistes. Certains experts américains imaginent que de telles stratégies de désinformation électronique pourraient être engagées à grande échelle soit par des États étrangers, soit même par des groupes criminels organisés afin de perturber la vie sociale et économique d'un pays. En 1980, le responsable des questions de sécurité au Stanford Research Institute (SRI), Donn B. Parker, avait ainsi mis en garde contre les effets déstabilisants qui pourraient affecter la sécurité nationale des États-Unis en cas de perturbation organisée du système de transfert de fonds électroniques ou des outils informatiques de comptabilisation de la masse monétaire [117]. Le développement du commerce électronique sur l'Internet accroît encore ce type de risques.

L'ensemble de ces menaces – techniquement similaires à celles qui affectent les systèmes d'information privés, mais susceptibles de porter des coups très durs à la capacité d'action et de défense des États – justifie actuellement la priorité donnée dans la plupart des pays développés à une politique de sécurité des systèmes sensibles et stratégiques et à la mise en place de règles spécifiques de protection de leur intégrité et de leur confidentialité. À travers celles-ci se met ainsi en place une sorte de *« secret de défense informatique »* [118], dont les incidences et les interactions avec les moyens de sécurité privés sont assez complexes à analyser.

La mise en place de règles spécifiques applicables aux systèmes informatiques et de communication

Le dispositif juridique et administratif assurant la sécurité des traitements et des données sensibles comporte – au-delà des dispositions pénales de droit commun réprimant la fraude informatique [119] – plusieurs volets : une adaptation des règles de protection du secret de défense en matière informatique, une réglementation particulière couvrant la cryptologie et la définition de normes de sécurité applicables aux systèmes d'information.

Les règles de protection du secret en informatique

Les risques et les particularités des systèmes d'information nécessitaient la définition de règles spécifiques pour la protection du secret en milieu informatisé. Cela a été entrepris depuis près de vingt ans sous la forme d'une adaptation des règles générales de protection plutôt que par la conception de logiques de protection totalement originales.

---

effectuer en précipitation une opération financière qui se retournera contre lui, dès que la véritable nouvelle sera connue.

[117] Donn B. Parker, *The Potential Effects of Electronic Fund Transfer Systems on National Security*, (dactyl.) SRI International, juin 1980.

[118] Cf. B. Warusfel, *Défense nationale*, *op. cit.*, p. 93.

[119] Le nouveau Code s'est contenté, pour l'essentiel, de réécrire légèrement la rédaction des infractions créées par la loi du 5 janvier 1988 sur la fraude informatique, qui sont désormais intégrées au nouveau Code sous les articles 323-1 à 323-7 nCP, auxquels s'ajoute l'article 226-15 nCP sanctionnant les atteintes au secret des correspondances *« émises, transmises ou reçues par la voie des télécommunications »* (cf. notamment Bertrand Warusfel, « Les technologies de l'information dans le Nouveau Code pénal », *Droit de l'Informatique et des Télécoms*, 94/2).

S'appliquent donc les différents principes généraux de la protection du secret aujourd'hui définis par le décret du 17 juillet 1998 : classification des supports, habilitation des personnes, protection des sites. Pour autant, des difficultés d'application pratiques apparaissent à ces trois niveaux, que les règles administratives (tels principalement l'instruction n° 1900 sur la protection du secret de défense en informatique) cherchent à prendre en compte :

– en ce qui concerne la classification des documents, l'immatérialité des supports informatiques et électroniques rend inefficace l'effet pédagogique et juridique du marquage ;

– en ce qui concerne l'habilitation des personnes, l'interconnexion des réseaux crée le risque permanent de l'accès à l'information d'une personne non autorisée ;

– en ce qui concerne la protection des sites, les systèmes d'information – notamment lorsqu'ils sont en réseau – paraissent très vulnérables physiquement et difficiles à surveiller d'un bout à l'autre des liaisons de communication.

Ces différents problèmes, qui fragilisent considérablement l'efficacité des règles traditionnelles de protection du secret, ne peuvent pas trouver de solution isolément. Ils impliquent un renforcement global de la sécurité des systèmes utilisés pour traiter les informations confidentielles et une grande rigueur dans les procédures entourant leur mise en œuvre.

L'effet recherché au travers des outils et des procédures de sécurité va être d'isoler, plus ou moins complètement, les systèmes d'information sensibles par rapport à l'extérieur et d'empêcher que des utilisateurs non autorisés puissent y accéder ou, pour le moins, puissent prendre connaissance de la partie confidentielle des données traitées. Les précautions à prendre concernent notamment *« l'identité de l'utilisateur,* (le) *travail en monoprogrammation et mono application et, éventuellement, l'isolement physique de l'ordinateur par rapport aux réseaux informatiques auxquels il est connecté »* [120].

Et ces mesures sont renforcées dans le cas particulier (et essentiel) de la transmission d'informations sensibles, voire classifiées. Suivant les cas, elle sera, soit totalement interdite, soit nécessairement effectuée en utilisant des moyens de chiffrement spécifiquement autorisés (cf. infra).

S'il est difficile de donner plus de précision sur les règles de protection des informations classifiées en milieu informatisé (car il s'agit d'un domaine qui fait l'objet de règles – elles-mêmes – fortement classifiées), il est cependant possible de se référer, par comparaison, aux recommandations édictées par l'administration en ce qui concerne le traitement informatique des *« informations sensibles ne relevant pas du secret de défense »* [121].

Ces recommandations constituent, en effet, en matière informatique, une autre forme de ces modes de protection périphériques du secret de

---

[120] Cf. B. Warusfel, *Défense nationale, op. cit.*, p. 93.

[121] Recommandation SGDN/DISSI/SCSSI n° 600, *op. cit.* Ce concept d'informations « sensibles mais ne relevant pas du secret de défense » s'inspire de la pratique administrative américaine qui avait projeté différentes restrictions (fort critiquées par la communauté scientifique américaine) concernant l'accès aux informations *« sensitive but un-classified »* (cf. *Washington Post*, 13 novembre 1986 ; *Documentaliste/Sciences de l'information*, n° 4/5, juillet 1985, p. 193).

défense, que nous avons déjà identifiés précédemment (cf. supra). Elles s'appliquent ainsi aux *« informations ne relevant pas du secret de défense, mais dont la destruction, la falsification, le détournement ou l'utilisation frauduleuse porterait atteinte aux intérêts nationaux, au patrimoine scientifique et technique, ou à la vie privée ou professionnelle des individus »* [122].

Les principales règles décrites dans ce document concernent, notamment :

– la responsabilisation et le contrôle hiérarchique des utilisateurs (avec signature d'un engagement de responsabilité);

– la sécurité physique des systèmes (protection contre le vol, l'intrusion, les risques accidentels) et les contrôles d'accès aux sites;

– la manipulation, la conservation et l'archivage des supports informatiques dans des lieux protégés;

– la définition et la gestion de droits d'accès et de niveaux d'habilitation entre les utilisateurs;

– la nécessité d'une authentification de l'utilisateur avant toute utilisation d'un poste de travail;

– une gestion rigoureuse des logiciels utilisés et leur vérification périodique;

– l'interdiction de transmettre des données sensibles sur une liaison sans que celle-ci ait été, au préalable *« approuvée »* (c'est-à-dire des liaisons dont les extrémités et les points de coupure sont en zone contrôlée) ou que soit utilisé – conformément à la réglementation en vigueur – un moyen de chiffrement approprié;

– la définition de certaines procédures de sauvegarde et de secours en cas d'incident.

On voit donc bien que la protection du secret de défense et des autres secrets de la nation dans un environnement informatisé (ce qui devient le cas le plus fréquent) nécessite des procédures adaptées, mais aussi que celles-ci doivent s'appuyer sur la mise en œuvre d'outils techniques de sécurité particuliers. C'est pourquoi les règles de protection sont complétées dans ce domaine par des règles spécifiques relatives à la cryptologie et à la sécurité des systèmes.

Le contrôle de la cryptologie et son évolution actuelle

L'usage du chiffrement comme moyen de sauvegarde de la confidentialité de l'information est un moyen très ancien [123]. Mais il a pris une

---

[122] *Ibid.*, p. 3. On reconnaît dans cette énumération la notion de *« patrimoine »*, une formule sur les *« intérêts nationaux »* (qui préfigure, là aussi, les *« intérêts fondamentaux de la nation »*) et une référence à la protection de la vie privée qui ne doit pas surprendre, étant donné que la loi du 6 janvier 1978 impose, dans son article 29, une obligation particulière de sécurité aux responsables de fichiers de données nominatives (désormais sanctionnée par l'art. 226-17 nCP).

[123] Parmi la littérature abondante sur les origines et le développement historique de la cryptologie, on se réfèrera notamment à André Lange & E.-A. Soudart, *Traité de cryptographie*, Alcan, 1935, pp. 13-92; J. W. Thompson & S. K. Padover, *L'espionnage politique en Europe de 1500 à 1815*, Payot, 1938, pp. 244-255; Fletcher Pratt, *Histoire de la cryptographie*, Payot, 1940 et pour des ouvrages plus récents : David Kahn, *La guerre des codes secrets - des hiéroglyphes à l'ordinateur*, Interéditions, 1980 (traduction française incomplète de *The Codebreakers*, Macmillan Co., New-York, 1967); Edmond Lerville, *Les cahiers secrets de la cryptographie*, Éditions du Rocher, 1972.

importance nouvelle avec deux vagues successives d'innovations technologiques. La première fut consécutive à l'apparition des télécommunications (sous leurs deux formes : filaires et par radio). Dès 1891, le règlement télégraphique international interdisait, par exemple, l'usage de *« lettres secrètes »* dans le contenu des télégrammes [124], prouvant ainsi indirectement l'importance qu'a revêtue dès ce moment la maîtrise par le pouvoir politique et les autorités militaires de l'usage des moyens de chiffrement. La seconde mutation technologique essentielle dans le domaine est venue du développement exponentiel des moyens informatiques, ce qui a, tout à la fois, accru les capacités de chiffrement (en termes de rapidité et de niveau cryptologique) et celles de décryptage [125].

Dans ce contexte technologique marqué par le développement des réseaux de communication et par la puissance croissante des moyens de calcul et de traitement, certains États n'ont pas renoncé à tenter de faire valoir leurs droits à l'usage et au contrôle de l'outil cryptologique. La plupart maintiennent des contrôles sur l'exportation de produits de cryptologie (dans le cadre des réglementations sur le contrôle des exportations à double usage, cf. supra). Mais en France, le contrôle gouvernemental s'est exercé, jusqu'à présent non seulement sur l'exportation mais également sur le commerce et l'usage de ces systèmes sur le territoire national. Le système de contrôle actuellement en vigueur repose sur les dispositions de la loi du 29 décembre 1990, ultérieurement complétées et modifiées par la loi du 26 juillet 1996. Mais ce dispositif devrait être prochainement revu.

Le contrôle institué par la loi de décembre 1990

C'est, en effet, la loi du 29 décembre 1990 sur la réglementation des télécommunications qui a prévu dans son article 28 le principe d'un régime juridique contraignant pour l'utilisation, la fourniture et l'exportation de moyens et de prestations de cryptologie. Elle a posé le principe (qui demeure inchangé sous l'empire de la loi de 1996) de la distinction entre deux types de procédure (déclaration préalable ou autorisation préalable) suivant le type de moyen (c'est-à-dire d'équipement) ou de prestation concernée, en énonçant que la fourniture et le commerce de ces moyens ou prestations sont soumis alternativement :

– à un contrôle par voie de déclaration préalable pour les activités touchant les moyens ou prestations qui ne peuvent avoir *« d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis »* [126] ;

---

[124] Ce règlement fut confirmé en France par un courrier du directeur des postes et télégraphes n° 229 du 7 avril 1892 (reproduit in Marquis de Viaris, *L'art de déchiffrer les dépêches secrètes*, Gauthier-Villard & fils/G. Masson, Paris, 1892, pp. 88 à 95). Cette prohibition de l'usage de la cryptologie dans les correspondances télégraphiques serait, cependant, tombée rapidement en désuétude.

[125] Rappelons-nous que les premiers ordinateurs au monde ont, d'ailleurs, été conçus pour réaliser le déchiffrement des codes ennemis durant la seconde guerre mondiale (notamment, la « Bomba » et « Colossus », machines réalisées en Grande-Bretagne sur les instructions du mathématicien Alan Thuring. Cf. notamment K. Flamm, *Creating the Computer - government, Industry and High Technology*, The Brookings Institution, Washington, 1988, pp. 34 à 39).

[126] Article 28.I. a) de la loi du 29 décembre 1990 avant modification.

– à un contrôle par voie d'une demande d'autorisation préalable (et, donc beaucoup plus contraignant et restrictif) pour les activités concernant les autres moyens ou prestations de cryptologie (c'est-à-dire, ceux qui assurent réellement une fonction de confidentialité).

Ces deux niveaux de procédure constituaient, à l'époque un effort d'assouplissement et de clarification notable par rapport à la situation antérieure à 1990 [127]. Précédemment, en effet, tous les systèmes cryptographiques étaient considérés comme des matériels de guerre et soumis sur le territoire national comme pour leur exportation aux dispositions du décret-loi de 1939 (cf. supra). Les rigueurs de cette réglementation n'avaient été que tardivement adoucies en février 1986 s'agissant des systèmes cryptologiques à usage commercial ou privé qui pouvaient – au cas par cas – faire l'objet d'une procédure assouplie [128].

Depuis 1990, la perspective a été renversée : d'une situation où la règle était l'application du régime des matériels de guerre et l'exception *« l'exclusion du régime des matériels de guerre »* de certains matériels commerciaux, on est passé à une situation dans laquelle les moyens de cryptologie ne sont plus des matériels de guerre, sauf dans le cas particulier de moyens de cryptologie *« qui sont spécialement conçus ou modifiés pour permettre ou faciliter l'utilisation ou la mise en œuvre des armes »* [129].

La logique de cette réforme de 1990 – et notamment celle sous-tendant la distinction entre moyens de chiffrement et moyens d'authentification – était claire : faciliter l'usage de la cryptologie commerciale dans les cas nécessaires tout en dissuadant, autant que faire ce peut, les personnes privées de se doter de véritables moyens de chiffrement des communications, et cela afin de conserver aux services officiels chargés d'effectuer les interceptions dans le cadre de la loi du 10 juillet 1991 la possibilité de les réaliser avec le maximum de succès. Dès lors, la voie déclarative – beaucoup moins contraignante – visait à orienter les entreprises vers l'utilisation de moyens cryptologiques limités aux seules fonctions d'authentification et de garantie d'intégrité [130].

Un décret et deux arrêtés du 28 décembre 1992 précisèrent les conditions pratiques du déroulement des procédures de déclaration et d'autorisation, tant pour la fourniture et l'utilisation en France que pour l'exportation. Ils confiaient au Service Central de la Sécurité des Systèmes d'Information (SCSSI) la responsabilité de recevoir, d'étudier et de statuer – au nom du Premier ministre, dont il dépend – sur les demandes d'autorisation qui lui sont présentées, y compris à l'exportation.

---

[127] Cf. E. Meillan, *op. cit.*, pp. 157 à 163.

[128] Décret n° 86-250 du 18 février 1986 portant modification du décret n° 73-364 du 12 mars 1973 relatif à l'application du décret-loi du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, auquel s'ajoutent deux arrêtés du 18 février 1986 relatif à la fabrication, au commerce, à l'acquisition, à la détention et à l'utilisation de moyens de cryptologie destinés à des fins professionnelles ou privées sur le territoire national, *JORF*, 26 février 1986, pp. 3018-3019 et p. 3022.

[129] Article 28.VI de la loi n° 90-1170 du 29 décembre 1990 (tel que modifiée en 1996). L'article 10 du décret du 28 décembre 1992 ne mentionnait, précédemment, que les moyens *« conçus ou modifiés pour les besoins militaires »* (*JORF*, 30 décembre 1992, p. 17915).

[130] On a assisté – dans un contexte juridique différent – aux mêmes tentatives aux États-Unis, où la NSA a cherché – sans succès – à écarter l'utilisation de l'algorithme RSA (qui permet à

Le développement de la controverse sur la légitimité du contrôle

Mais l'un des principaux problèmes provoqués par l'application de cette procédure de contrôle de la cryptologie restait son antinomie, au nom de l'intérêt public de la sécurité nationale, avec l'autre intérêt public qui veut que les entreprises et les particuliers puissent développer la sécurité de leurs propres patrimoines. Certes, dans ce domaine, la doctrine juridique internationale respecte les droits de l'État à limiter les libertés individuelles et économiques au nom de la sécurité nationale [131]. Mais en freinant l'accès des entreprises à l'achat et l'utilisation des produits de chiffrement, la législation française (comme d'une manière différente, la législation américaine et ses règles de restriction à l'exportation) avait cependant choisi en 1990 d'opposer la protection du secret de défense et celle du secret commercial privé. La querelle qui s'engagea aux États-Unis en 1994 autour du système *Clipper* (un algorithme de chiffrement contenu dans un processeur spécialisé dont les autorités fédérales pourraient obtenir les clés afin d'en déchiffrer les messages) a, finalement, contribué à mettre le débat sur la place publique [132].

Les prises de position en faveur d'une libéralisation des conditions d'utilisation de la cryptologie se sont alors fait de plus en plus fréquentes, tant au niveau français [133] qu'international. Ainsi, dans son projet de Livre vert sur la sécurité des systèmes d'information, la Commission des Communautés européennes a souhaité dès 1993 que s'instaure – au minimum – une complémentarité entre les besoins de sécurité commerciaux et ceux qui relèvent de la protection du secret de défense [134]. Plus directement, la Chambre de commerce internationale (CCI) prit position en faveur d'une libéralisation des outils de cryptologie en faveur des entreprises [135].

Enfin, l'OCDE a directement choisi de soutenir un développement de l'utilisation de la cryptologie qui respecterait les prérogatives des États, en publiant en 1997 des lignes directrices qui ont explicitement pour but de *« promouvoir l'utilisation de la cryptographie »* et de *« contribuer à assurer la sécurité des données, et à protéger la vie privée »* tout en évitant

---

la fois la signature et le chiffrement) en proposant le DSA (Digital Signature Standard), un standard de signature qui ne pouvait pas servir de moyen de chiffrement.

[131] C'est ainsi que les lignes directrices adoptées par l'OCDE en matière de sécurité des systèmes précisent qu'elles *« n'affectent pas les droits souverains des États en ce qui concerne la sécurité nationale et l'ordre public, lesquels demeurent régis par la législation nationale »*. Cependant le même texte souligne que *« les parties doivent notamment s'efforcer d'éviter que la situation n'évolue dans le sens d'une approche dualiste avec, d'un côté, un régime applicable aux systèmes d'information en rapport avec la sécurité nationale et, de l'autre, des règles concernant tous les autres systèmes d'information »* (OCDE, *Lignes directrices régissant la sécurité des systèmes d'information*, 26 novembre 1992).

[132] Cf. notamment *Le Monde*, 22 et 23 juillet 1994, et pour une réaction hostile au sein de la communauté américaine de l'informatique, Mike Godwin, « A Chip Over My Shoulder : The Problems with Clipper », *Internet World*, juillet/août 1994, pp. 92 à 95.

[133] Cf. notamment, Paul Vidonne, « Pour une vraie liberté de crypter », *Le Monde*, 15 mai 1996; Jean Guisnel, « Plaidoyer pour la liberté de crypter », *Expertises des systèmes d'information*, janvier 1996, p. 13.

[134] Commission des Communautés Européennes, DG XIII, *Green Book on the Security of Information Systems* (Draft 3.6.), 14 juillet 1993, p. 11.

[135] Cf. « Prise de position de la CCI sur une politique internationale de chiffrement » *in Droit de l'Informatique et des Télécoms*, 94/2, pp. 70 à 74.

de *« mettre indûment en péril la sécurité publique, le respect des lois et la sécurité nationale; ... »* [136].

L'assouplissement du contrôle par la loi de 1996 et l'échec des « tiers de séquestre »

La loi du 26 juillet 1996 modifiant la réglementation des télécommunications n'a pas remis en cause le principe du contrôle par l'État de la fourniture et du commerce de la cryptologie. Elle a maintenu l'obligation de déclaration pour la fourniture et le commerce des moyens ou prestations qui n'assurent pas de fonction de confidentialité [137] et l'obligation d'une autorisation préalable lorsqu'il s'agit de moyens ou de prestation qui assurent de telles fonctions [138]. Tout au plus, la nouvelle rédaction du texte a-t-elle apporté quelques modifications secondaires, qui n'en ont pas changé la philosophie même si elles ont pu s'avérer d'une grande portée pratique [139].

Le point le plus important fut qu'à partir de cette loi de 1996, le contrôle de la cryptologie a cessé d'être exhaustif, puisqu'elle prévoyait que le gouvernement définissait par voie réglementaire les conditions dans lesquels certains moyens ou prestations peuvent faire l'objet d'une dispense totale de toute formalité préalable, lorsque leurs *« caractéristiques techniques ou (leurs) conditions d'utilisation sont telles que ces opérations ne sont pas susceptibles de porter atteinte aux intérêts mentionnés au deuxième alinéa* (c'est-à-dire les intérêts nationaux ou de sécurité des communications) » [140]. De même, des textes réglementaires pouvaient aménager des procédures simplifiées ou encore prévoir le déclassement d'un moyen ou d'une prestation de cryptologie du régime d'autorisation vers le régime déclaratif.

Des assouplissements importants ont donc été introduits quant à l'utilisation des moyens et des prestations de cryptologie. La loi de 1996 a ainsi créé deux cas de totale liberté d'utilisation, ce qui était – dans son principe – une importante innovation.

Le premier cas de liberté d'utilisation concerna tous les moyens ou prestations qui n'assurent pas de fonction de confidentialité (c'est-à-dire, tous ceux qui sont soumis – en ce qui concerne leur fourniture et leur commerce – au régime déclaratif) : *« L'utilisation d'un moyen ou d'une prestation de cryptologie est : a) Libre : (...) si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis »* [141]. Cela signifie que tout moyen ou prestation n'assurant pas de chiffrement (mais

---

[136] OCDE, *Lignes directrices régissant la politique de cryptographie*, 27 mars 1997.

[137] Article 28.I.2° b) de la loi du 29 décembre 1990, tel que modifiée par l'article 17 de la loi du 26 juillet 1996.

[138] Article 28.I.2° a) de la loi du 29 décembre 1990 modifiée.

[139] Cf. notamment, Bertrand Warusfel, « Les conditions juridiques de la sécurité sur l'Internet et le régime de la cryptologie en France » in Association Française du Droit de l'Informatique, *Internet saisi par le droit*, Éditions des Parques, 1997, pp. 205-211.

[140] Article 28.I.3° de la loi du 29 décembre 1990 modifiée.

[141] Article 28.I.1° a) de la loi du 29 décembre 1990 modifiée.

de la signature électronique, par exemple) dont la fourniture a été préalablement déclarée dans les règles (et a, donc donné lieu à la délivrance d'un récépissé de déclaration) a pu, dès lors, être acquis et utilisé sans aucune contrainte par tout utilisateur sur le territoire français [142].

Le second cas, en revanche, peut être aujourd'hui considéré comme n'ayant quasiment jamais reçu d'application pratique et donc obsolète. Il s'agissait d'accorder la liberté d'utilisation aux moyens ou prestations de chiffrement dont la fourniture aurait été préalablement autorisée et dont leurs conventions secrètes (c'est-à-dire, les clés servant au chiffrement) seraient détenues et gérées par un tiers de séquestre agréé [143] :

> *« l'utilisation d'un moyen ou d'une prestation de cryptologie est : a) Libre : (...) si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon les procédures et par un organisme agréés dans les conditions définies au II »* [article 28.I.1.a) modifié].

Ces tiers, chargés de séquestrer et de gérer les clés de chiffrement pour le compte des utilisateurs souhaitant bénéficier de la liberté d'utilisation, devaient recevoir un agrément préalable du Premier ministre [144] et accepter différentes contraintes, telles que l'assujetissement au secret professionnel, l'obligation de conserver les clés et – surtout – l'obligation de les remettre ou de les *« mettre en œuvre »* (c'est-à-dire de réaliser eux-mêmes le déchiffrement d'un message à partir de la clé séquestrée) lorsqu'une demande leur serait adressée par les autorités judiciaires ou administratives dans le cadre de la loi du 10 juillet 1991 réglementant les interceptions ou dans certains cas d'enquête préliminaire ou de flagrance [145].

Par ce *« compromis »* [146], l'État, assuré de pouvoir ainsi procéder rapidement et discrètement aux déchiffrements qu'il souhaite, pensait pouvoir contrebalancer la mise sur le marché des moyens de chiffrement de plus en plus performants que les entreprises attendaient. Mais le délai excessif qui sépara la loi de juillet 1996 de la parution de ses décrets

---

[142] Il ne s'agissait, en fait, là que de l'officialisation de la pratique antérieure puisque, conformément à l'article 2 alinéa 2 du décret du 28 décembre 1992, la déclaration d'utilisation personnelle n'avait déjà pas à être souscrite lorsque le moyen avait fait l'objet préalablement d'une déclaration d'utilisation générale.

[143] Cette technique du recours à un tiers permettant à l'État de procéder aisément au déchiffrement des messages interceptés pour des raisons judiciaires ou de sécurité nationale, avait été reconnue comme valable par les travaux de l'OCDE : *« Les systèmes de gestion de clés pourraient offrir une base pour une possible solution qui concilierait les intérêts des utilisateurs et ceux des organismes chargés de faire respecter la loi »* (OCDE, *Lignes directrices régissant la politique de cryptographie*, 27 mars 1997).

[144] *« Les organismes chargés de gérer pour le compte d'autrui les conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité doivent être préalablement agréés par le Premier ministre ».*

[145] Cf. l'article 28-II alinéas 1 à 5 de la loi du 29 décembre 1990 modifiée.

[146] Pour reprendre le terme employé par le général Desvignes, alors chef du SCSSI, dans un article où il présentait la philosophie des nouvelles dispositions comme *« un juste compromis entre la satisfaction d'un besoin indiscutable de sécurité au profit des libertés individuelles (le secret des informations médicales, par exemple) comme des intérêts économiques, industriels et financiers et la faculté, non moins indiscutable, pour les services de l'état et la Justice, de continuer à jouer leur rôle »* (Jean-Louis Desvignes, « La sécurité des systèmes d'information », *Défense*, n° 71, mars 1996, p. 66).

d'application, ainsi que la rigueur de certaines des obligations mises à la charge des tiers agréés ne permirent pas à cette solution médiane de s'imposer.

Le décret du 24 février 1998 précisa finalement les conditions et les conséquences de cet agrément des tiers chargés d'offrir le service de séquestre de clés [147]. Les deux éléments essentiels en étaient l'engagement de respecter un cahier des charges détaillé et la nécessité pour le candidat de *« compter, parmi ses personnels, un nombre de personnes habilitées pour être en mesure de satisfaire aux obligations du décret du 12 mai 1981 »* (art. 4). Cette exigence de bénéficier de personnels habilités au Secret-défense se comprenait puisque, par principe, tout ce qui concerne les interceptions de sécurité est classifié. Mais cette obligation d'habilitation, avec les délais qu'elle impliquait, ajoutée aux autres contraintes de la procédure d'agrément fut généralement considérée par le marché comme induisant des coûts excessifs qui ne pouvaient que dissuader les éventuels candidats au métier de tiers de séquestre. Effectivement, plus d'une année après la publication de ce décret d'application, seules deux entreprises de service avaient demandé et obtenu l'agrément.

Le 19 janvier 1999, le Premier ministre, M. Lionel Jospin annonça alors *« un changement fondamental d'orientation »*, reconnaissant que *« les dispositions issues de la loi de 1996 ne sont plus adaptées »* et proposant de *« rendre complètement libre l'usage de la cryptologie en France, tout en adaptant les moyens des pouvoirs publics pour garantir les libertés publiques dans ce nouvel environnement et pour lutter contre l'utilisation des moyens de chiffrement à des fins délictueuses »* [148]. La nouvelle politique annoncée s'articulerait autour de deux axes : *« offrir une liberté complète dans l'utilisation des produits de cryptologie, sous la seule réserve du maintien des contrôles à l'exportation découlant des engagements internationaux de la France »* [149] *»* et *« supprimer le caractère obligatoire du recours au tierces parties de confiance pour le dépôt des clefs de chiffrement ».*

Cette nouvelle politique s'est traduite immédiatement par l'adoption d'autres textes réglementaires mettant en œuvre une nouvelle étape de la libéralisation du commerce et de l'usage de la cryptologie [150]. Et la principale disposition de ces textes a été de ne plus soumettre la fourniture des produits de chiffrement n'utilisant pas une clé supérieure à 128 bits qu'à une simple déclaration auprès du SCSSI [151]. Par ailleurs, une nouvelle loi – modifiant sensiblement les dispositions de 1996 – a été annoncée, qui devrait poursuivre vers la voie d'une libéralisation encore plus large

---

[147] Cf. *JORF*, 25 février 1998, pp. 2915-2916.

[148] Cf. la déclaration du Premier ministre reproduite in *Droit & Défense*, n° 98/4, p. 77.

[149] C'est-à-dire le maintien d'un contrôle des exportations de moyens de chiffrement utilisant des clés supérieures à 56 bits, conformément aux engagements pris au sein de l'Arrangement de Wassenaar et retranscrits dans la liste de contrôle des biens à double usage publiée par l'Union européenne (cf. supra).

[150] Décret n° 99-199 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation ; Décret n° 99-200 du 17 mars 1999 les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable ; Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie (*JORF* du 19 mars 1999, pp. 4050-4053).

[151] Cf. Marie Pasquier « Une étape importante dans la libéralisation de la cryptologie », *Droit & Défense*, n° 99/1, pp. 72-73.

de l'usage de la cryptologie et revoir sensiblement à la baisse le statut et le rôle des tiers de séquestre. En contrepartie, ce nouveau texte va sans doute renforcer les pouvoirs de l'État en ce qui concerne la remise du contenu clairs des messages chiffrés interceptés ou découverts lors d'une perquisition.

La définition de normes de sécurité des systèmes

Si dans le domaine de la cryptologie, l'intérêt public qui s'attache à la protection des communications gouvernementales et à la possibilité de réaliser des *« interceptions de sécurité »* (pour emprunter la terminologie de la loi française du 10 juillet 1991) paraît partiellement contradictoire avec les intérêts privés de protection des secrets concurrentiels, il est un autre aspect de la politique de sécurité informatique gouvernementale qui ne pose pas les mêmes problèmes de principe. Il s'agit de la définition de normes techniques spécifiant des systèmes informatiques sécurisés. Dans ce domaine, comme dans beaucoup d'autres en ces matières, les États-Unis sont la puissance initiatrice et dominante.

La première de ces normes a été celle qui est relative à la lutte contre les *« rayonnements compromettants »*. Il semble, en effet, que les Américains aient observé, dans les années cinquante, des effets parasites sur leur nouvelle machine à chiffrer SIGTOT, qui consistaient en une sorte d'écho électromagnétique (qui furent dénommés *« transients »* ou encore *« artifacts »*) répercutant sur la ligne de transmission sur laquelle circulait le message chiffré l'image du texte original introduit « en clair » dans la machine. Ils découvrirent ensuite que les systèmes soviétiques souffraient des mêmes faiblesses (ce qui permit des interceptions fort importantes, notamment concernant les projets militaires soviétiques durant la guerre de Corée [152]). Une fois analysé scientifiquement, il fut attesté que tout système électronique était susceptible d'émettre deux sortes de signaux électromagnétiques parasites : d'une part un rayonnement radioélectrique, de l'autre un phénomène de conduction (renvoyant une onde électromagnétique par le biais d'une ligne électrique ou de transmission reliée au système) [153]. Et il fut établi qu'une fois identifiés et captés, ces signaux pouvaient être *« compromettants »* (c'est-à-dire qu'ils pouvaient – convenablement traités – permettre de reconstituer plus ou moins précisément le traitement d'information en cours sur le système émetteur) [154]. Des exemples d'interception de ce type ont été, d'ailleurs, évoqués publiquement, que ce soit dans le domaine de l'espionnage commercial [155], ou de l'espionnage militaro-stratégique [156].

---

[152] Cf. D. C. Martin, *op. cit.*, pp. 104 et 105. L'amiral Klotz estimait, pour sa part, que cette menace électromagnétique a été prise en compte *« à partir des années 60 »* (Commission Nationale Informatique et Libertés, Annexe 18, « Audition de M. l'Amiral Bernard Klotz, délégué interministériel à la sécurité des systèmes d'information », *Rapport annuel 1987*, p. 225).

[153] Cf. Colonel René Gasser, « L'informatique : des systèmes protégés contre les fuites », *Armées d'Aujourd'hui*, n° 116, décembre 1986/janvier 1987, p. 21.

[154] Cf. notamment, en ce qui concerne le rayonnement compromettant engendré par les écrans d'ordinateur, W. Van Eyck, « Rayonnement électromagnétique d'information par des terminaux cathodiques », *Actes du Congrès Sécuricom 1985*, p. 299.

[155] Un cas d'espionnage électronique par captation des radiations électromagnétiques au détriment d'une société du secteur électrique aurait été découvert en Italie (Cf. *AFP*, 1er mars 1989).

[156] L'ancien directeur de la DST a révélé que ce service aurait neutralisé, par exemple, deux agents soviétiques sous couverture diplomatique, en train de se livrer dans un parking proche

C'est pourquoi le Département de la défense adopta finalement une norme technique fixant les niveaux de rayonnement maxima à ne pas dépasser pour qu'un système soit réellement anti-compromettant. Il s'agit du *National Communication Security Information Memorandum* (NACSIM) *5100A*, norme classifiée adoptée par la NSA [157]. Ce standard américain, adopté par les principaux pays alliés des États-Unis (l'OTAN en a établi une version propre sous la référence ASMG 720B) est communément connu sous le nom de norme *Tempest* (*« Transient Electromagnetic Pulse Emanation Standard »*). Les autorités françaises s'y réfèrent également [158], au travers d'une instruction interministérielle n° 300, établie par le SCSSI.

Le principe est donc que les informations classifiées les plus confidentielles ne peuvent être traitées que par des systèmes d'information protégés contre ces rayonnements compromettants. Deux moyens principaux s'offrent alors techniquement pour parvenir à ce niveau de discrétion des systèmes [159]. Le premier s'applique principalement aux sites importants (sites militaires lourds, ambassades situées dans des pays sensibles, ...) : il consiste à installer les systèmes à protéger à l'intérieur d'une « cage de Faraday » afin d'empêcher toutes fuites électromagnétiques. Le second moyen réside dans l'utilisation d'ordinateurs conçus et montés spécialement pour réduire les risques de compromission. Ces systèmes « blindés » et conformes à la norme *Tempest* sont principalement fabriqués par les grands constructeurs américains (qui proposent des versions sécurisées de leurs gammes civiles) ou par certains sous-traitants spécialisés aux États-Unis. Ces systèmes sont soumis, tant aux États-Unis qu'en France, à des contraintes à l'exportation ainsi qu'à des autorisations gouvernementales en ce qui concerne leur utilisation par les organismes publics.

Par ailleurs, au-delà de l'aspect des protections techniques, la doctrine considère aujourd'hui que les dispositions pénales relatives à la fraude informatique (telles qu'elles sont désormais reprises dans le nouveau Code pénal) rendent la *« captation de signaux parasites exploitant l'effet Tempest (...) parfaitement incriminable. Si, un jour, les tribunaux répressifs devaient être saisis d'un tel dossier, ils trouveraient dans l'arsenal juridique existant le moyen de sanctionner de tels agissements »* [160].

Le deuxième type de normes apparues plus récemment en matière de sécurité des systèmes et de protection du secret en informatique, concerne la définition d'architectures logicielles de sécurité. La sauvegarde des informations classifiées à l'intérieur des bases de données informatiques nécessite, en effet, que les logiciels d'exploitation de ces systèmes répondent à certains critères, en ce qui concerne notamment le contrôle d'accès, la séparation des différents fichiers au sein de la base, ou encore le suivi et l'enregistrement de toutes les opérations réalisées par les utilisateurs.

---

d'un site du CEA, à des interceptions électromagnétiques visant un système informatique de la Direction des applications militaires (cf. Marcel Chalet & Thierry Wolton, *Les visiteurs de l'ombre*, Grasset, 1990, p. 135).

[157] Cf. notamment James B. Schultz, « Defeating Ivan with TEMPEST », *Defense Electronics*, juin 1983, pp. 64 à 75.

[158] Cf. R. Gasser, *op. cit.*, p. 21.

[159] Cf. notamment *Info-DGA*, n° 27, avril/mai 1990, p. 33.

[160] Michel Vivant, « Les captations illicites des signaux parasites sous le coup de la loi pénale », *Droit et Défense*, 94/3, p. 8.

Là encore, le Département de la défense américain et le centre de sécurité informatique de la NSA ont été les pionniers avec la publication en 1983 d'un document connu depuis lors sous le nom familier d'*« Orange Book »* [161]. Il établit des critères qui *« constituent un jeu cohérent d'exigences de base et de niveaux d'évaluation pour certifier l'effectivité des contrôles de sécurité implantés dans les systèmes de traitement automatisé d'information. Ces critères sont conçus pour être utilisés dans l'évaluation et la sélection de systèmes d'information intervenant dans le traitement et/ou le stockage et le retrait d'informations sensibles ou classifiées par le Département de la défense »*.

La mise en œuvre des méthodes et des critères définis dans cet *Orange Book*, a créé un premier cadre normalisé pour la définition de systèmes d'information adaptés aux exigences de la protection du secret, et particulièrement des données classifiées. En revanche, ce document a paru insuffisant car il ne traitait que des aspects de confidentialité (à l'exclusion de l'intégrité et de la disponibilité) et qu'il ne paraissait pas aisé de concilier cette approche à usage gouvernemental avec celles utilisables pour les entreprises privées [162]. D'autre part, les pays européens se sont émus du monopole américain dans ce domaine [163] et la Commission des Communautés européennes a fait approuver dans le même domaine un document rédigé à l'origine par quatre pays européens (France, Grande-Bretagne, Allemagne et Pays-Bas) les « ITSEC. » (Information Technology Security Evaluation Criteria) [164], tandis que les principaux pays occidentaux impliqués dans ces questions (les États-Unis, le Canada et les quatre Européens précités) ont établi des *« critères communs »* permettant la reconnaissance mutuelle des certifications de sécurité effectuées sur la base des documents américains, canadiens ou européens [165].

---

[161] Department of Defense, Computer Security Center, *Department of Defense Trusted Computer System Evaluation Criteria*, CST-STD-001-83, 15 août 1983.

[162] Cf. « Controverses autour du critère du DoD », *Sécuritique*, n° 4, septembre 1987, p. 4. Pour une synthèse sur l'Orange Book, cf. Hubert Macé, « Critères d'évaluation au Département de la Défense des États-Unis », *Normatique*, n° 31, novembre 1991, pp. 2-3.

[163] *« Les États-Unis délivrent des certificats de sécurité, mais ils ne les délivrent qu'aux entreprises américaines. Il y a par conséquent un problème pour les entreprises européennes »* (entretien avec J. Vincent-Carrefour, *Les cahiers de la sécurité intérieure*, *op. cit.*, p. 113).

[164] Cf. Recommandation du Conseil du 7 avril 1995 concernant des critères communs d'évaluation de la sécurité des technologies de l'information, *JOCE*, L 93 du 26 avril 1995, pp. 27-28.

[165] Cf. notamment, Daniel Martin, *La criminalité informatique*, PUF, 1997, pp. 107-108.